Iira Hakola

Pilvipohjaiset langattomat lähiverkot

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

28.11.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Iira Hakola Pilvipohjaiset langattomat lähiverkot 50 sivua + 1 liite 28.11.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Lehtori Jukka Louhelainen

Työssä tutustuttiin Cisco Systemsin, AeroHive Networksin ja Aruba Networksin pilven kautta hallittaviin tukiasemiin, pilvihallinta-alustoihin, ja niiden teknisiin ominaisuuksiin. Työn tavoitteena oli selvittää jokaisen tutkitun kokonaisuuden tekniset ja totutukselliset erot ja selvittää, mikä näistä kolmesta yrityksestä kannattaa valita verkon toteuttamiseksi. Työssä tulee myös esille pilvipohjaisen verkkoratkaisun edut. Työn teon yhteydessä Metropolia Ammattikorkeakoululle tilattiin opetuskäyttöön neljä kappaletta Ciscon MR42-tukiasemia, minkä ansiosta Ciscon Meraki-alustaa oli mahdollista käyttää. AeroHiven ja Aruban tukiasemiin ja alustoihin tutustuttiin yritysten tarjoaman dokumentaation kautta.

Työssä käydään ensin läpi Ciscon MR42-tukiaseman tekniset ominaisuudet ja yrityksen käyttämät ratkaisut. Seuraavaksi käydään läpi kaikki Meraki-alustan toteutukseen liittyvät ominaisuudet, eli miten verkon ja laitteiden konfigurointi tehdään ja millä tavoilla alusta esittää verkosta kerättyä dataa. AeroHiven ja Aruban osalta laitteiden ominaisuudet ja tapa, jolla verkko konfiguroidaan kummankin yrityksen alustoilla, käydään läpi niin tarkasti kuin mahdollista yritysten tarjoaman dokumentaation avulla. Kummastakin yrityksestä kerrotaan ensin, mitä yhtäläisyyksiä kaikista tutkituista tukiasemista ja alustoista löytyy, ja yritysten omat ratkaisut käydään läpi samoin kuin Ciscon kohdalla.

Lopuksi työssä kootaan yhteen kaikki yritysten ratkaisuihin liittyvät vahvuudet ja heikkoudet, sekä verrataan niitä toisiinsa. Yritysten tuotteita mietitään myös siltä kannalta, mikä niistä kannattaisi valita verkon toteuttamiseen. Tutkinnan perusteella AeroHiven tuotteiden ominaisuudet todettiin parhaiksi kaikista kolmesta, Ciscon alusta helpoiten käytettäväksi. Aruban tuotteet jäävät jälkeen kummassakin. Viimeinen päätelmä on, että se, mistä tuotteet tilataan, tulee valita verkon vaatimusten perusteella, jolloin kukin yritys voi silti olla sopiva vaihtoehto. Työssä tutkitut tekniset ominaisuudet ja alustat osoittavat, että pilvipohjaisen verkkoratkaisun valitseminen kannattaa, vaikka verkon voisi edelleen toteuttaa fyysistä kontrolleria käyttäen.

Avainsanat	pilvi, tukiasemat, Cisco, AeroHive, Aruba, WLAN, langaton lähiverkko

Author(s) Title Number of Pages Date	Iira Hakola Cloud controlled wireless local area networks 50 pages + 1 appendix 28 November 2016
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networking
Instructor(s)	Jukka Louhelainen, Senior Lecturer

This study researches the technical features and implementation choices of cloud controlled access points and cloud based management platforms from Cisco Systems, AeroHive Networks and Aruba Networks. The goal was to define the technical and implementational differences of each solution, in consideration of which of the three options would be the choice for network implementation. the study also explores the advantages of a cloud controlled wireless networks. While the study was conducted Metropolia University of Applied Sciences ordered four of Cisco's MR42 -access points for education purposes, which enabled the use of Cisco's Meraki platform in the research. AeroHive's and Aruba's platforms and access points were studied through their documentation as best as possible.

The technical features of the MR42 -access point are explained first and then the study goes through every implementation feature, i.e. how a network is configured and how data is displayed, in the Meraki platform. For AeroHive and Aruba the features and configuration options are explained as well as possible by studying their documentation. The similarities are listed first and then all of their unique solutions are explained in detail.

In the summary all the discussed strengths and weaknesses of all three solutions are compiled and compared. The systems are also compared for the purpose of concluding which one of them is best for network implementation. Based on the study AeroHive's products' features are the most advanced, Cisco's platform is the easiest to use, and Aruba falls behind in both aspects. The final conclusion is that the choice is to be made based on the needs of the planned network, which is why each choice can be suitable. The studied technical features and the platforms clearly indicate that in any case choosing a cloud controlled network solution is beneficial, despite the fact that implementations which use physical controllers are still very common.

Keywords	cloud, access points, Cisco, AeroHive, Aruba, WLAN, wireless local area network

Sisällys

1 Johdanto.

Insinöörityön tarkoitus on tutustua Cisco Systemsin, AeroHive Networksin ja Aruba Networksin tarjoamiin pilvipohjaisiin verkonhallinta-alustoihin ja pilven kautta hallittaviin tukiasemiin. Alustojen ja tukiasemien ominaisuudet ja toteutus käydään läpi mahdollisimman tarkasti niin, että jokaisen yrityksen vaihtoehtoja voisi verrata keskenään parhaimman vaihtoehdon löytämiseksi. Työn teon yhteydessä Metropolia Ammattikorkeakoululle tilattiin opetuskäyttöön neljä kappaletta Ciscon Meraki-sarjan MR42-tukiasemia, joten Ciscon alustaa on mahdollista tutkia lähemmin. AeroHiven ja Aruban alustoihin tutustutaan molempien yritysten dokumentaation ja konfigurointiohjeiden kautta. Tukiasemista tutkitaan niitä tukiasemia, jotka olivat uusimpia jokaisen yrityksen valikoimassa. Työn alkaessa Ciscon MR42-tukiasema oli yrityksen uusimpia, mutta Cisco on myöhemmin julkaissut uusia malleja.

Ensimmäiset yritysluokan tukiasemat olivat standalone-tukiasemia, toisin sanoen autonomisia eli itsenäisiä. Nämä tukiasemat eivät kommunikoi lainkaan toistensa kanssa, ja jokainen niistä täytyy konfiguroida erikseen. [1.] Standalone-tukiasemissa ei myöskään ole ohjaustasoa [2, s. 6] ja niiden kaistanleveys sekä hallinta- ja suojausominaisuudet on rajoitettu. Standalone-tukiasemien ongelmien ratkaisuksi kehitettiin fyysinen kontrolleri, joka toimii keskitettynä ohjaus- ja datatasona, ja sen avulla myös tukiasemat voidaan konfiguroida keskitetysti. Kontrollerin käyttö vaatii tukiasemilta ominaisuuksia, joita standalone-tukiasemissa ei ole. Näitä tukiasemia kutsutaan kevyiksi tukiasemiksi (Lightweight Access Point, LWAP), ne ovat fyysisesti kevyempiä kuin standalone-tukiasemat, ne voi liittää verkkoon Power over Ethernet -kytkennällä (PoE) [1], ja esimerkiksi Ciscon LWAP:lla on useita eri toimintatiloja, kuten tila, jossa tukiasema voi olla yhteydessä kontrolleriin WAN-linkin kautta, ja tila, jossa tukiasema valvoo verkkoa hyökkäyksiltä [3]. Tämä ns. keskitetty malli sisältää kuitenkin vielä lukuisia ongelmia. Jos tukiasemat menettävät yhteyden kontrolleriin, koko verkko kaatuu, ja datatason tunnelointi yhteen kohteeseen muodostaa pullonkaulan. Kontrollerit pystyvät tukemaan vain tiettyä määrää tukiasemia, jolloin aina kun kontrollerin kapasiteetti täyttyy, on pakollista ostaa uusi kontrolleri, ja usean kontrollerin hallitseminen saattaa vaatia ylimääräistä hallinta-sovellusta. [2, s. 7.] Kontrollerin rajoituksia on yritetty poistaa virtualisoinnin ja integroinnin avulla. Virtualisoinnin ansiosta tarvittavan muistin ja porttien määrää voi lisätä tarpeiden mukaan. Myös tukiasemien toimintaa muutettiin tässä vaiheessa niin, että dataa voidaan

siirtää paikallisesti tukiasemien välillä. Muita ratkaisuja on kontrollerin integroiminen esimerkiksi kytkimiin ja palomuureihin. Myös tukiasema saattoi toimia kontrollerina joukolle muita tukiasemia.

Lähivuosina verkonhallinta on muuttunut pilvipalveluksi. Osassa ratkaisuista itse kontrolleri toimii nyt pilven kautta palveluntarjoajan tiloissa, kun taas jotkin yritykset ovat kehittäneet tuotteitaan niin pitkälle, että kontrolleria ei enää tarvita ollenkaan. Niissä palveluissa, joissa käytetään kontrolleria, tukiasemat ovat edelleen osittain riippuvaisia kontrollerista: yhteyden katkeaminen palveluun tuottaa edelleen ongelmia verkon toiminnan, palveluiden ja esimerkiksi suojauksen kanssa. [2, s. 8.] Ratkaisuissa, jossa kontrolleria ei enää ole, ohjaus- ja datatasot kulkevat nyt suoraan tukiasemien välillä. Vain laitteiden hallinta on keskitettyä, ja tukiasemat ovat tarpeeksi tehokkaita suorittamaan ne toiminnot, joihin kontrolleria tarvittiin aikaisemmin. Tämänlaiset ratkaisut yksinkertaistavat verkon toimintaa ja ovat entistäkin skaalautuvampia ja joustavampia. Aikaisempien ongelmien lisäksi uusissa ratkaisuissa on otettu huomioon verkkojen muuttuneet vaatimuksen. Nykyaikana jopa yritysverkkojen täytyy tukea lukemattomia mobiililaitteita, työntekijöiden ja vierailevien henkilöiden kannettavista tietokoneista bluetooth-laitteisiin. [2, s. 9.] Samalla myös itse verkon hallinta on noussut uuteen avainasemaan. Yritykset, jotka tarjoavat pilven kautta toimivia laitteita, tarjoavat myös niiden hallintaan räätälöityjä alustoja, jotka toimivat suoraan selaimen kautta ilman asennusta. Alustoilla on mahdollista konfiguroida laitteet helposti valikoiden kautta, hallita laitteita, suorittaa vianhakua, ja ylläpitäjä saa kokonaisvaltaisen kuvan verkon tapahtumista sekä radioympäristöstä tukiasemista kerättävän datan ansiosta.

2 Cisco Meraki

Meraki on Ciscon pilvipohjainen verkonhallinta-alusta ja sarja tukiasemia, kytkimiä ja muita verkkolaitteita. Työssä käsitellään Merakin ominaisuudet mahdollisimman tarkasti Ciscon dokumentaation pohjalta ja tutkitaan itse hallinta-alustaa. Metropolia Ammattikorkeakoululle tilattiin neljä kappaletta Ciscon MR42-tukiasemia, jotka kytkettiin koulun verkkoon, mikä mahdollisti hallinta-alustan ominaisuuksien tutkimisen ympäristössä, jossa laitteet ovat toiminnassa ja keräävät dataa verkon toiminnasta.

Meraki-palvelut sijaitsevat ympäri maailmaa useassa Ciscon datakeskuksessa, joista jokaisella on tier-1 SAS70 type II/SSAE 16 -sertifikaatti. Datakeskusten kohdalla on otettu

huomioon palveluiden toimivuus, suojaus ja varotoimet ongelmien sattuessa. Ciscon mukaan Meraki-palvelut toimivat 99,99 % ajasta, joka vastaa alle yhden tunnin mittaista katkosta vuoden aikana. Palveluiden toimivuutta pidetään silmällä vuorokauden ympäri, ja kaikki asiakkaiden data on kopioitu kolmelle itsenäiselle datakeskukselle. Fyysisten vikojen sattuessa kaikki asiakasdata siirretään välittömästi varalla oleviin laitteisiin eivätkä mahdolliset katkot vaikuta itse asiakkaan verkon toimintaan. Datakeskuksien verkot ja tilat on suojattu uhkien varalta, sekä luonnonkatastrofeja vastaan. Verkkoja valvotaan tunkeutumisilta ympäri vuorokauden, ne on suojattu IP- ja portti-pohjaisilla palomuureilla, ja etäyhteys on rajoitettu IP-osoitteen perusteella ja se vahvistetaan RSA-avaimella. Pääsy jokaiseen datakeskukseen on suojattu kortinlukijoilla ja biometrisillä lukijoilla. Kaikkien sisään- ja ulospääsyjen ja kaappien luota löytyvät valvontakamerat ja vartijat, jotka valvovat kulkua sisään ja poistumista keskuksista ympäri vuorokauden. Keskukset on suunniteltu suojaamaan laitteita tulipalon, sähkökatkon ja maanjäristyksen sattuessa. Jos käy niin, että jokin datakeskuksista ei enää pysty ylläpitämään palveluita, ne siirretään toiseen maantieteellisesti muualla sijaitsevaan datakeskukseen. [4.]

Ciscon out-of-band control -ohjaustaso huolehtii asiakkaiden verkon toimivuudesta silloinkin, kun yhteys Meraki-pilveen on katkennut. Ohjaustaso erittelee Meraki-laitteiden hallintaan liittyvän datan ja asiakkaiden käyttäjädatan toisistaan. Hallintadata kulkee asiakkaiden laitteista Meraki-pilveen suojattua internetyhteyttä pitkin, kun taas asiakkaan verkon käyttäjien data, esimerkiksi internetsivujen selaus ja yrityksen sisäiset sovellukset, kulkevat suoraan kohteeseensa LAN:in tai WAN:in kautta (Local Area Network, Wide Area Network). Jos yhteys pilveen katkeaa, suurin osa laitteiden ominaisuuksista toimivat lukuun ottamatta konfigurointi- ja diagnostiikka-työkaluja, ja splash-sivuja (luku 3.2). Jos WAN-yhteys on käytössä, myös yhteys internetiin säilyy. [5.]

MR42-tukiaseman tekniset tiedot:

- Kaksi asiakasradiota: 2,4 GHz radio 802.11b/g/n standardien laitteille ja 5 GHz radio 802.11a/n/ac standardien laitteille.
- Maksimidatanopeus 1,9 Gbit/s.
- Dual-band radio WIDS/WIPS-tekniikoille (luku 2.3), spektrianalyysille ja sijaintianalyysille.
- 2,4 GHz Bluetooth Low Energy (BLE) lähetys ja skannausradio (luku 3.2).
- Integroidut ja suuntaamattomat antennit.

- 3x3:3 MIMO kolmella spatiaalisella (avaruudellisella) virralla, SU-MIMO ja MU-MIMO tuki (luku 2.1).
- 20 ja 40 MHz:n kanavat 802.11n standardille ja lisäksi 80 MHz kanava 802.11ac standardille.
- Molemmat 2,4 GHz:n ja 5 GHz:n alueet pystyvät käyttämään 256-QAM modulaatiota. [6, s. 8.]

Seuraavissa luvuissa syvennytään tarkemmin tukiasemissa käytettyihin ratkaisuihin, tekniikoihin ja ominaisuuksiin.

2.1 802.11ac Wave 2

Ciscon Meraki-tukiasemat hyödyntävät 802.11ac Wave 2 -nimen saanutta IEEE-standardia, joka on päivitys vuonna 2013 julkaistuun alkuperäiseen ac-standardiin. Yksi tärkeimpiä ac-standardiin tehtyjä lisäyksiä on tuki MU-MIMO (Multi User Multiple-input-multiple-output) tekniikalle, joka toimii yhdessä beamforming-tekniikan kanssa [4]. Alkuperäinen MIMO tai SU-MIMO (Single User Multiple-input-multiple-output), on tekniikka, jonka avulla tukiasema voi lähettää dataa yhdelle käyttäjälle usean antennin kautta. MU-MIMO:n ajatus on muuten samanlainen, mutta nyt dataa voidaan lähettää usealle käyttäjälle. [8.] 802.11ac wave 2 -standardi on rajoitettu niin, että tukiasema voi kommunikoida yhtäaikaisesti korkeintaan neljän asiakkaan kanssa, kahdella datavirralla kullekin asiakkaalle [7].

Olennainen osa varsinkin MU-MIMO:n toimintaa on beamforming, jonka avulla tukiasema ja tietty asiakaslaite voivat ohjata signaaleja suoraan toisiaan kohti, ja näin vahvistaa lähetyksen tehoa. SU-MIMO:n kanssa beamforming vahvistaa signaalien voimakkuutta ja nostaa bittinopeutta. MU-MIMO:n kanssa beamforming pitää huolen siitä, että asiakkaat vastaanottavat heille tarkoitettua signaalia. Esimerkiksi, jos vastaanottajia on kolme, käyttäjälle yksi osoitettua signaalia vahvistetaan ja suunnataan oikeaan osoitteeseen, kun samalla signaalia ohjataan muualle avaruuteen niin, että se ei kulje kahden muun vastaanottajan suuntaan. [8.] MIMO tarvitsee toimiakseen vielä MRC-tekniikkaa (Maximal Ratio Combining). Koska MIMO:n avulla vastaanotetaan dataa usealla antennilla, jokainen antennin vastaanottama signaali on eri vaiheessa ja niillä on eri amplitudi. MRC on algoritmi, jonka avulla vastaanotetut signaalit voidaan muokata yhdeksi vahvistetuksi signaaliksi muuttamalla niiden vaihetta ja amplitudia yhtenäisemmäksi [9, kaavio

2]. MU-MIMO toimii vain toisten sitä tukevien laitteiden kanssa. Tällä hetkellä se on mahdollistettu vain yhteen lähetyssuuntaan eli tukiasemalta käyttäjälle [7].

2.2 BYOD ja Systems Manager

Ciscon Bring Your Own Device -ratkaisu on kehitetty nykyaikaisia langattomia verkkoja varten, missä käyttäjien omistamien laitteiden määrä on kasvanut räjähdysmäisesti. Ratkaisun tarkoitus on tehdä verkon valvonta ja suojaus helpoksi silloin, kun verkkoon liittyy uusia laitteita ja käyttäjiä päivittäin. Useat Ciscon Meraki-tukiasemien hallintaliittymän ominaisuudet tukevat tällaisia verkkoja. Tukiasemat käyttävät integroitua sovelluskerroksen sormenjälkitunnistustekniikkaa (kerros 7, L7), jonka avulla hallintajärjestelmä näyttää ja luokittelee kaikki havaitut käyttäjälaitteet. Laitteiden luokittelun ansiosta käyttäjille on esimerkiksi mahdollista asettaa ryhmäkäytäntöjä automaattisesti luokan mukaan. Verkon suojausta on helppo vahvistaa network access control -ominaisuudella (NAC), joka antaa vain niiden laitteiden liittyä verkkoon, joissa on virustentorjuntaohjelma. Hallinta-alustan verkonvalvonta-ominaisuudet keräävät tietoa verkkoon liittyneistä laitteista ja raportoi jokaisen laitteen siirtämän datan määrän. [10.] Tukiasemat käyttävät sormenjälkitunnistusta myös liikenteen tutkimiseen, ja verkon kapasiteetin riittävyys on varmistettu Auto RF- ja traffic shaping -ominaisuuksilla. [11.]

Ciscon Systems Manager (SM) on Enterprise Mobility Management -alusta (EMM) mobiililaitteiden hallintaa varten. EMM-alustat tukevat käyttäjälaitteiden hallintaa tavallisten BYOD-ominaisuuksien ohella. [10; 12.] Meraki-laitteet tukevat Systems Managerin käyttöä automaattisesti, mutta jotta alustan saa käyttöön, sitä varten täytyy luoda tili erikseen samalla tavalla kuin hallintaliittymän käyttöä varten [13]. Alustasta ei myöskään ole saatavilla täyttä versiota ilman lisenssiä. Ilmainen versio sallii enintään sadan laitteen hallinnan eikä versiolle ole tarjolla puhelintukea. Alustalle voi ostaa lisenssin sen mukaan, kuinka monta laitetta sillä haluaa hallita, ja lisenssiin sisältyy ympärivuorokautinen puhelin- ja sähköpostituki. [14.] SM-alustaa käytetään Merakin Dashboard-hallintaliittymän kautta, jossa se toimii omana SM-verkkonaan [13]. SM-verkon käyttäminen on helppo tapa lisätä verkon turvallisuutta riippuen tavasta, jolla laite liittyy SM-verkkoon ensimmäisen kerran SM-komponentit ja määritetyt profiilit sekä sovellukset asennetaan laitteeseen automaattisesti tai manuaalisesti. Suojausta voi lisätä myös käyttämällä käyttäjien

todennusta verkkoon liittymisen yhteydessä. [12.] Asennettavat profiilit sisältävät ne asetukset, jotka laitteelle halutaan määrittää. Profiileissa voi olla esimerkiksi seuraavanlaisia asetuksia:

- Rajoitukset: Systems Managerilla on mahdollista rajoittaa esimerkiksi elokuvia, TV-ohjelmia ja sovelluksia kaistan säästämiseksi.
- Pääsykoodi: Pääsykoodia käytetään lukitun laitteen avaamiseen. Koodin yhteydessä voi määrittää esimerkiksi koodin tyypin, vahvuuden, ja sen, milloin laite lukitaan. [12.]
- WiFi: WiFi-asetuksilla voidaan esimerkiksi liittää laitteeseen WPA2-Enterprise-todennus. [15.]
- Data Leakage Protection (DLP): DLP on suojaus tietovuotoja vastaan, jolla voi esimerkiksi estää epäluotettavaksi luokiteltujen kolmannen osapuolen tarjoamien sähköpostisovellusten käytön [12].

Laitteet ryhmitellään sovelluksien ja asetuksien jakamista varten merkintöjen avulla. Merkinnät voivat olla automaattisia, jotka usein määräytyvät laiteominaisuuksien, kuten laitteen käyttöliittymän perusteella tai ylläpidon manuaalisesti luomia ja asettamia. Merkintöjä voi asettaa myös käyttäjille, milloin kyseinen merkintä pätee kaikkiin niihin laitteisiin, jotka tämä käyttäjä on liittänyt SM-verkkoon. [12.]

2.3 Air Marshal

Air Marshal on Ciscon oma WIDS/WIPS (Wireless Intrusion Detection System/Wireless Intrusion Prevention System) alusta langattomien uhkien estämistä varten. MR42-mallissa Air Marshal toimii yhdessä tukiasemaan asennetun 2,4 ja 5 GHz:n alueilla yhtä aikaa toimivan (dual-band) radion kanssa, jonka tehtävä on havaita langattomia uhkia. Jokainen Ciscon tukiasemista sisältää Air Marshal -alustan, mutta kahdessa ulkokäyttöön tarkoitetuista malleista (MR62, MR66) ei sisällä äsken mainittua dual-band WIDS -radiota. Jos yrityksen valitsema tukiasema-malli ei sisällä Air Marshal -alustan käyttöön erikseen tarkoitettua dual-band-radiota, niin verkko voidaan skannata uhkien löytämiseksi vain kerran päivässä tai silloin, kun tukiasemalla ei ole käyttäjiä. Sen lisäksi, että tukiasema skannaa ympäristön silloin kuin se voi, se voidaan määrittää tekemään pakollinen skannaus kerran päivässä. Jos yrityksen verkko vaatii tehokkaampaa valvontaa, nämä tukiasemat voidaan asettaa tilaan, jossa ne eivät ole ollenkaan asiakkaiden käytössä, vaan laitteen molempia radioita käytetään verkon kokoaikaiseen valvontaan. Samat ominaisuudet löytyvät myös tukiasemista, joissa on kolmas radio, mutta niiden

käyttö ei ole välttämätöntä, koska kolmas radio skannaa verkkoa ympäri vuorokauden häiritsemättä tukiaseman läpi kulkevaa liikennettä [16, s. 10].

WIDS ja WIPS alustana Air Marshalin toiminta jakautuu kahteen pääosaan: verkon valvontaan ja uhkien hallintaan. Air Marshal jakaa uhat seuraaviin kategorioihin:

- Luvattomat SSID:t: Luvattomat tukiasemat voivat tekeytyä toiseksi tukiasemaksi kopioimalla toisen tukiaseman verkon SSID:n tai naamioitua kokonaan toiseksi tukiasemaksi kopioimalla SSID:n lisäksi myös BSSID:n, jolloin luvatonta tukiasemaa on mahdotonta erottaa siitä tukiasemasta, joksi se on naamioitunut. Molemmista tapauksista käytetään nimitystä spoofing. Jos luvattoman tukiaseman mainostama verkko näkyy myös lankaverkossa, niin lankaverkko on mahdollisesti vaarassa.

- Muut SSID:t: Lähistöllä olevat muut langattomat verkot saattavat aiheuttaa radiotaajuushäiriötä yrityksen verkossa. Lisäksi modernit älypuhelimet ja mobiililaitteet pystyvät mainostamaan WiFi-verkkoja eteenpäin muodostaen Ad-Hoc-verkon (verkkoalue jossa laitteet keskustelevat vain keskenään ilman tukiasemaa) muiden mobiililaitteiden kanssa. Tämä ns. langaton silta voi toimia yhdyskäytävänä langattomille hakkereille.

- Haitalliset broadcastit: DoS-hyökkäys (Denial of Service, palvelunestohyökkäys) on yritys estää käyttäjiä saamaan yhteys tiettyyn palveluun, tai tässä yhteydessä tiettyyn tukiasemaan/tukiasemiin. Hyökkäys toimii niin, että käyttäjille lähetetään suuri määrä broadcast-tyyppisiä viestejä, jolloin verkon toiminta hidastuu tai katkeaa kokonaan.

- Packet floods, ”pakettitulvat”: DoS-hyökkäyksen lisäksi Air Marshal huomioi muut verkossa liikkuvat suuret pakettimäärät, vaikka kyseessä ei olisikaan DoS-hyökkäys. Paketit ryhmitellään vielä niiden tyypin perusteella.

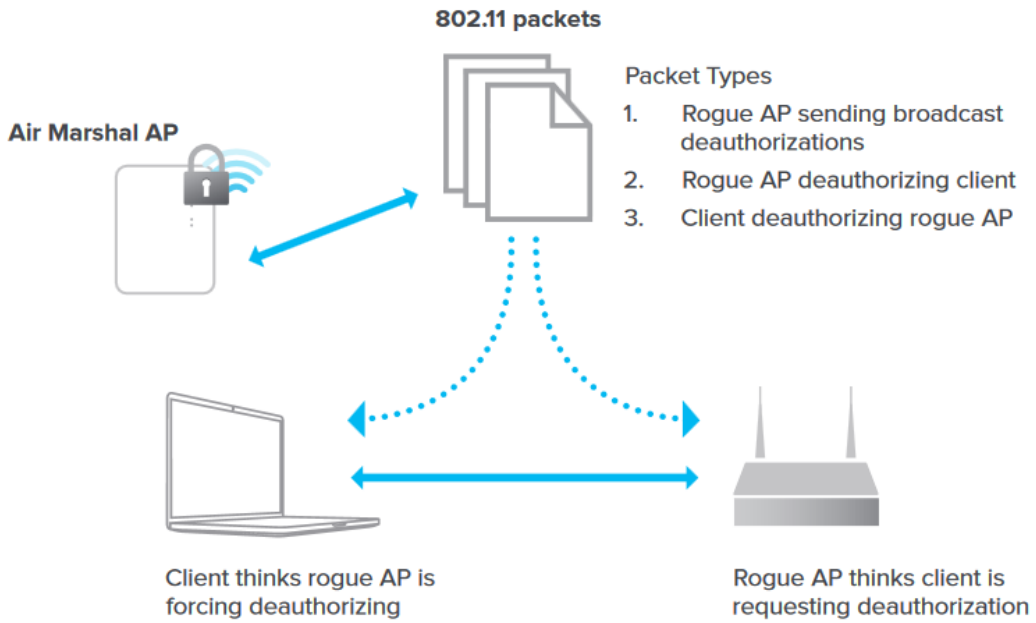
- Käyttäjien ”harhailu”: Yritykseen kuuluvat laitteet saattavat vahingossa liittyä verkkoon, joka ei ole yrityksen oma tai sen hyväksymä. Tämä on erityisen vaarallista, jos kyseessä on aiemmin mainittu kopioitu SSID tai naamioitunut tukiasema.

Näiden uhkien lisäksi Air Marshal huomioi myös PCI DSS:n (Payment Card Industry Data Security Standard) asettamat vaatimukset jälleenmyyjille koskien sellaisia ympäristöjä, joissa luottokorttitietoja käsitellään ja siirretään WLAN-verkossa. [16, s. 5-6.]

Air Marshal käyttää dual-band-radiota langattoman verkon skannaamiseen löytääkseen mahdollisia luvattomia tukiasemia tai muita uhkia. Langattoman verkon lisäksi Air Marshal tutkii myös sitä käyttävän laitteen lankaverkkoon liitetyn portin läpi kulkevan liikenteen nähdäkseen, onko siihen liitetty ulkopuolisia tukiasemia. Vielä näiden lisäksi yritys voi valvoa heille tärkeitä laitteita (kannettavat tietokoneet, myymäläympäristön laitteet kuten kassakoneet ja viivakoodinlukijat yms.) sen osalta, mihin langattomaan verkkoon

ne ovat yhdistyneenä. Näiden laitteiden ei koskaan tulisi yhdistyä mihinkään muuhun kuin yrityksen omaan verkkoon niiden sisältämien tietojen vuoksi. Verkon ylläpitäjälle lähetetään sähköposti-ilmoitus havaituista ongelmista hänen määrittämiensä parametrien mukaisesti. [16, s. 7.]

Air Marshal -alusta kykenee hallitsemaan havaittuja langattomia uhkia automaattisesti. Uhka hallitaan matkimalla kyseistä tukiasemaa tai naamioitumalla kyseiseksi tukiasemaksi, ja saattamalla se toimintakyvyttömäksi. Luvattomalle tukiasemalle lähetetään iso määrä 802.11-protokollan paketteja käyttäen sen BSSID-osoitetta (Basic Service Set Identifier, sama kuin MAC-osoite) pakettien lähdeosoitteena. Toinen, tehokkaampi, tapa hallita uhkia on tehdä naamioituminen ns. ”kahteen suuntaan”. Tämä tarkoittaa, että luvattoman tukiaseman lisäksi Air Marshal naamioituu myös laitteiksi, jotka yrittävät yhdistyä uhkaavan tukiaseman tarjoamaan verkkoon ja lähettää paketteja käyttäen myös näiden laitteiden lähde MAC-osoitetta. Kuva 1 havainnollistaa tätä prosessia: luvattomaksi tukiasemaksi naamioitunut Air Marshal lähettää broadcast-viestinä (paketti joka lähetetään kaikille tiettyyn ryhmään kuuluville jäsenille) luvattomaan verkkoon paketin valtuutuksien poistosta. Broadcast-viesti laukaisee prosessin, jossa käyttäjälaitteet luulevat, että itse luvaton tukiasema pakottaa valtuutuksien poiston, ja vastaavasti luvaton tukiasema luulee, että käyttäjälaite pyytää valtuutuksien poistoa. Tämän seurauksena molemmat osapuolet katkaisevat yhteyden toisiinsa. Cisco haluaa Air Marshalin käyttäjän huomioivan, että tämä prosessi kaataa kohdeverkon täysin, jonka takia sitä tulisi käyttää äärimmäisellä varovaisuudella ja vain viimeisenä vaihtoehtona. [16, s. 8.]



Kuva 1. Luvattoman tukiaseman hillitseminen havainnollistettuna [16, sivu 8].

Ciscon Meraki-dokumentointi ja Air Marshal -datalehdet antavat käyttäjälle kattavat ohjeet alustan tehokasta käyttöä varten. Dokumentteihin liitetyt esimerkki kuvat on kuitenkin otettu ennen Meraki Dashboardin viimeisintä visuaalista päivitystä, jonka vuoksi voi olla suositeltavaa ottaa käyttöön Dashboardin vanha näkymä.

2.4 Mesh-ominaisuudet

Mesh-verkko on verkko, jossa useat tukiasemat keskustelevat keskenään langattomasti. Ne muodostavat yhden verkon, jossa suurin osa tukiasemista ei ole kiinni lankaverkossa. Mesh-verkko sopii tiloihin, joihin on vaikeaa tai liian kallista asentaa Ethernet-kaapelointia, ja ne ovat erittäin vikasietoisia. Meraki-tukiasemat tukevat mesh-ominaisuutta automaattisesti ilman, että laitteita tarvitsee konfiguroida mesh-verkon luontia varten. [17.] Mesh-tukiasemilla voi olla kaksi eri roolia: yhdyskäytävä ja toistin (repeater). Yhdyskäytävän toimiva tukiasema on liitetty suoraan lankaverkkoon ja se toimii käytävänä internetiin. Toistimena toimiva tukiasema ottaa yhteyden yhdyskäytävä-tukiasemaan mesh-linkin avulla ja saa internetyhteyden tätä kautta. Mesh-linkki muodostuu niin kauan, kuin toistimella on vahva yhteys toiseen toistimeen tai yhdyskäytävään. Jos yhdyskäytävä menettää internetyhteyden, laite varmistaa ensin, että lähistöllä on toinen yhdyskäytävä-tukiasema, jolla on internetyhteys, ja toimii siitä eteenpäin toistimena. [18.]

Mesh-verkon tukiasemat keskustelevat keskenään Ciscon oman reititys-protokollan avulla. Kyseinen protokolla ja muut Ciscon kehittämät algoritmit arvioivat linkkien toimivuutta mittaamalla esimerkiksi signaalin vahvuutta, suoritustehoa, muiden laitteiden aiheuttamia häiriöitä, ja vastaanotettujen pakettien määrää. Myös kapasiteettia ja käyttäjien suoritustehoa optimoidaan tarvittaessa reitittämällä liikennettä eri kanavien kautta. Mesh-verkko pitää itseään yllä vikatilanteissa: verkko konfiguroituu uudelleen itsestään, sillä tukiasemat siirtävät liikenteen toimiville tukiasemille tunnettujen linkkien kautta. [17.] Mesh-verkkoa voi valvoa wireless > access points -sivulta Dashboard-hallintaliittymässä. Sivu näyttää tukiasemien tuntemat reitit, mesh-naapurit, ja linkkien suoritustehon. Tunnetuista reiteistä kerrotaan liikenteen määrä reittiä kohden ja reitin metri, joka muodostetaan pudonneiden pakettien määrästä ja pakettien lähetysajasta. Suoritusteho-graafi kuvaa linkin toimivuutta tasaisin väliajoin suoritettavan suoritustehotestin perusteella. [18.]

2.5 Muita ominaisuuksia

Ciscon CMX Location Analytics on ratkaisu, joka on kehitetty keräämään tietoa tietyn verkon alueella liikkuvista WiFi-laitteista. Ratkaisun tarkoitus on antaa ylläpidolle, tai vaikka liiketilojen omistajalle, parempi kuva käyttäjien läsnäolosta verkossa. Havaitut laitteet jaotellaan ohikulkijoihin ja vierailijoihin, minkä tarkoitus on havaita esimerkiksi muutoksia verkon käyttöasteessa pitkin päivää tai sesonkien mukaisia muutoksia, ja kertoa, kuinka kauan käyttäjät viettävät keskimäärin aikaa verkossa ja kuinka usein he vierailevat verkossa. [19, luku 3.] Kaappausaste (Capture Rate) on prosentuaalinen määrä ohikulkijoista, joista tuli vierailijoita. Ohikulkijat ovat laitteita, jotka tukiasema on havainnut vähintään kerran. Ohikulkijoista tulee vierailijoita, kun laite on ollut havaittuna viisi minuuttia ja sessio aloitetaan, kun laitteesta saadun signaalin suhteellinen voimakkuus (RSSI, Received Signal Strength Indication) on vähintään 15. Sessio jatkuu niin kauan, kun RSSI on jatkuvasti kymmenen tai enemmän. Sitoumus kertoo minuutteina, kuinka kauan vierailija viettää verkon alueella ja lojaalius kertoo, kuinka usein sama käyttäjä vierailee verkossa. [19, luku 3, kaavio 2.] CMX API (Application Programming Interface, ohjelmointirajapinta) on valinnainen lisäominaisuus CMX sijainti analyysi alustalle, jossa kerättyä dataa ei analysoida ja esitetä Dashboardissa. Se lähetetään organisaation määrittämälle palvelimelle reaaliaikaisesti HTTP-protokollan avulla. [19, luku 4.1.]

Meraki-tukiasemista löytyvä kolmas radio, ja sisäänrakennettu spektrianalysaattori, valvovat ja analysoivat verkkoa automaattisesti kellon ympäri verkon suorituskyvyn maksimoimiseksi [20; Liite 1]. Radio mittaa 2,4 GHz:n ja 5 GHz:n taajuuskanavien käyttöä, lähellä olevien tukiasemien aiheuttamia häiriöitä ja käyttäjälaitteiden ominaisuuksia. Spektrianalysaattori mittaa muiden laitteiden, kuten Bluetooth-laitteiden ja mikroaaltouunien, aiheuttamia häiriöitä ja lataa nämä tiedot pilveen. Kun tukiasema tekee automaattisia muutoksia radioiden toimintaan, se käyttää pilveltä löytyviä algoritmeja, jotka on luotu yli 15000 verkon tietojen pohjalta, sekä tukiasemista kerättyä reaaliaikaista ja historiallista dataa sopivien asetusten löytämiseksi. Tukiasema voi vaihtaa käytettäviä taajuuskanavia sekä radioiden lähetystehoa ja ohjata käyttäjiä taajuuskanavalta toiselle. [Liite 1.] Spektrianalysaattoria käytetään myös verkkoympäristöstä kerätyn datan visualisoimiseen hallinta-alustassa [21].

Layer 7 sormenjälkitunnistus -tekniikkaa käytetään myös sovelluksiin liittyvän liikenteen palvelunlaadun parantamiseen. Merakin Layer 7 -teknologia on tätä tarkoitusta varten räätälöity datapaketteja käsittelevä ”moottori”, mikä suorittaa sovellusliikenteen hallintaa tehokkaasti tuoteperheiden sisällä ja tuotteista riippuen. Teknologian avulla on mahdollista tunnistaa ja hallita satoja sovelluksia. Tunnistus mahdollistaa esimerkiksi VoIP-liikenteen priorisoinnin samalla, kun paljon kaistaa käyttäviä sovelluksia rajoitetaan tai estetään. Layer 7 -teknologia ja laitteiden sormenjälkitunnistus tuottavat myös hyödyllistä dataa Meraki-laitteiden hallinta-alustaan verkkoa eniten käyttävistä sovelluksista ja laitteista, mikä auttaa tunnistamaan, mitä rajoituksia liikenteelle tulisi asettaa. [22.]

3 Cisco Merakin pilvipohjainen hallinta

Meraki-laitteita ja -sovelluksia hallitaan Dashboard-sovelluksen kautta, joka on selainpohjainen graafinen käyttöliittymä (GUI, Graphical User Interface). Tässä luvussa keskitytään tukiasemien hallintaan Dashboardin kautta. Tukiasemia voi hallita myös laitekohtaisesti My Meraki -sivun kautta, josta kerrotaan lisää luvussa 3.3. Osalla kerrotuista tiedoista ei ole suoranaista lähdettä, vaan tiedot on kerätty Meraki-alustaa tutkimalla.

Kun tilatut laitteet on lähetetty, tilaaja saa sähköpostin, josta ilmenevät tilauksen tiedot, linkki Dashboard-sivulle sekä Dashboardin käyttöönottoon tarvittava lisenssiavain. Sovellukseen tehdään tunnukset käyttäjälle sekä se, kenellä on organisaation laajuiset ylläpitäjän oikeudet. Tämän jälkeen käyttäjä luo yrityksen ensimmäisen verkon ja lisää

verkkoon haluamansa laitteet. Tässä vaiheessa laitteet eivät vielä ole organisaation laiteluettelossa vaan ne pitää ensin lunastaa (claim). Lunastuksen voi tehdä samalta sivulta kuin laitteiden lisäyksen ja siihen tarvitaan joko laitteiden sarjanumero tai tilauksen numero. Kun laiteet on lunastettu ja lisätty, verkko on käytännössä valmis, koska laitteet toimivat oletusasetuksilla heti, kun ne on kytketty verkkoon. [23.]

Verkosta, jossa on vain tukiasemia, näkyy Koko verkko- ja Langaton-välilehdet (Network-wide, Wireless), jotka molemmat jakautuvat Valvonta- ja Asetukset-osioihin (Monitor, Configure). Organisaation ylläpitäjillä näkyy näiden lisäksi Organisaatio-välilehti (Organization), mistä löytyvät työkalut koko organisaation laajuiseen valvontaan ja lukuisien asetusten määrittämiseen. Ylläpitäjä näkee tältä välilehdeltä yleiskatsauksen organisaation verkoista ja lokin (Change log) muutoksista, joita muut ylläpitäjät ovat tehneet näissä verkoissa. Välilehdeltä voi esimerkiksi lisätä uusia organisaatio oikeuden omaavia ylläpitäjiä, muuttaa heidän oikeuksiaan, ja muokata kaikkiin ylläpitäjiin liittyviä turvakäytäntöjä. Asetuksista voi myös estää Merakin tuen pääsyn organisaatiosi tietoihin, hallita Merakin Mobiililaitteiden hallinta-sovelluksen (MDM, Mobile Device Management) sertifikaatteja, ja ottaa käyttöön ja konfiguroida SNMP-valvonnan. Tiedot yrityksen aktiivisista lisensseistä löytyy myös tältä välilehdeltä. [24.]

3.1 Verkon valvonta ja tilastot

Koko verkko -välilehdeltä (Network-wide) löytyvät seuraavat valvontatyökalut: käyttäjät, pakettien kaappaus, tapahtumaloki ja yhteenveto. Yhteenveto-sivu (Summary report) antaa kaikkein laajimman kuvan verkon käytöstä, sen käyttäjistä ja käyttäjien suosimista laitteista sekä sovelluksista. Verkossa liikkuneen datan määrä ja käyttäjien määrä päivää kohden on esitetty graafisesti. Eniten dataa käyttäneet tukiasemat, SSID:t, käyttäjät ja sovellukset on listattu taulukkona. Sivulta löytyy myös muita tietoaja, kuten käytön perusteella suosituimmat laitevalmistajat ja käyttöjärjestelmät. Verkossa liikkuneen datan määrä näkyy myös Käyttäjät-sivulta (Clients) ja Dashboardin etusivulta. Käyttäjät-sivulla näytetään tarkempaa tietoa verkon käytetyimmistä sovelluksista, joka näytetään ympyrädiagrammina, sekä yksityiskohtaisena taulukkona, joka aukeaa ympyrädiagrammin alta löytyvästä ”more>>”-painikkeesta. Ympyrädiagrammin sisällön voi myös vaihtaa kertomaan eniten käytetyistä porteista tai HTTP-liikenteen sisällöstä. Verkon käyttäjät on listattu yhteen taulukkoon, jossa näkyvät esimerkiksi käytetyn datan määrä, IP-osoite, ja käyttäjälle asetettu käytäntö.

Pakettien kaappaus (Packet capture) on työkalu, jolla voi tutkia verkon läpi kulkevia paketteja reaaliaikaisesti. Kaappausvaihtoehdot vaihtelevat hieman eri laitteiden välillä, tukiasemilla käytettävissä olevat vaihtoehdot ovat:

- Tukiasemat: Minkä tukiaseman tai tukiasemien liikennettä kaapataan.
- Kappauksen tyyppi: Liikennettä voi kaapata joko langattomasta yhteydestä tai lankaverkon yhteydestä.
- Ulostulo: Kaapattuja paketteja voi katsoa suoraan ko. välilehdellä tai kaappauksen voi ladata .pcap-tiedostona Wireshark-ohjelmaan.
- Suodatus: sovelluksen voi halutessaan käskeä sivuuttamaan broadcast- ja/tai multicast-liikenteen, ja sovellukselle voi määrittää suodatusehtoja.

Pakettien kaappausta voi käyttää yksityiskohtaisen tiedon hankinnassa esimerkiksi paikantaessa verkossa esiintyviä ongelmia tai antamaan kuva siitä, miten tietty tukiasema kommunikoi yrityksen lankaverkon kanssa. [25.] Toimintalokista (Event Log) voi tarkastella lukuisia verkon tapahtumia, mikä on vianhaun kannalta toinen erittäin hyödyllinen työkalu. Näkyviä lokitietoja voi rajata päivämäärän ja ajan, käyttäjän tai Meraki-laitteen, ja tapahtumatyypin perusteella. Tukiasemien osalta loki tallentaa seuraavat tapahtumat:

- Langattoman yhteyden muodostus ja katkaisu.
- WPA-todennus ja todennuksen purku yhteyden katkaisun yhteydessä.
- RADIUS todennus ja todennuksen purku yhteyden katkaisun yhteydessä.
- Splash-sivun kautta tapahtuneet todennukset.
- Air Marshalin suorittamat otolliset ja/tai pakolliset kanavien skannaukset.
- Tiedot laitteiden vaeltamisesta eri VLAN:ien välillä verkkokerroksessa (L3 roaming).
- Air Marshalin havaitsemat pakettitulvat.
- Dynaamiseen, eli automaattiseen taajuuskanavan vaihtoon (DFS, Dynamic Frequency Selection) liittyvät tapahtumat.
- Virtuaalisen yksityisverkon (VPN, Virtual Private Network) yhteyden katkeamiset ja muut yhteyteen liittyvät tapahtumat. [26.]

Langaton-välilehdeltä (Wireless) löytyy laaja kirjo erilaisia työkaluja tukiasemien kokonaisvaltaista valvontaa varten. Niitä ovat tukiasemat, kartta ja pohjapiirrokset, Air Marshal, sijaintianalytiikka, sijaintilämpökartta, PCI-raportti, Bluetooth-käyttäjät ja radiotaajuusspektri. Tukiasemat-sivu (Access points) näyttää listan verkossa olevista tukiasemista ja näyttää niistä käyttäjän valitsemat tiedot, kuten esimerkiksi laitteen ja yhteyden

tilan, MAC-osoitteen, hälytykset ja käyttöasteen. Sivua voi katsella järjestelmän uudella tai vanhalla näkymällä, joissa on hieman eroja. Vanhassa näkymässä käyttäjällä on enemmän ja eri vaihtoehtoja mistä valita, kun hän valitsee, mitä tietoja tukiasemasta näytetään. Laitteiden tilasta ilmoitetaan myös, onko tukiasema asetettu aktiiviseksi Air Marshal -skanneriksi, toisin kuin uudessa näkymässä. Tältä sivulta voidaan lisätä uusia tukiasemia, joka onnistuu myös etusivulta. Tietyn tukiaseman nimeä klikkaamalla pääsee katsomaan yksityiskohtaisia tietoja ko. tukiasemasta. Tätäkin sivua voi tarkastella järjestelmän uudessa tai vanhassa ulkoasussa.

Kartat ja pohjapiirrokset -sivu (Map & floor plans) näyttää organisaation käytössä olevat tukiasemat kartalla Google Mapsin avulla. Sama kartta on näkyvillä monella muullakin sivulla, kuten esimerkiksi etusivulla. Kartasta näkee nopeasti tukiasemien tilan, sillä niiden indikaattori vaihtaa väriä tai muotoa ko. tukiaseman tilan mukaan. Kartan päälle voi lisätä ja sijoittaa myös pohjapiirroksia, jos tukiasemien sijainti halutaan nähdä tarkemmin. Air Marshalin asetukset määritellään tämän osion Air Marshal -sivulta, eikä Asetukset-osiosta. Ylläpitäjä voi avainsanojen määrittää, mitkä verkot koetaan automaattisesti uhkiksi ja täten myös hillitään automaattisesti. Air Marshalin voi määrittää suorittamaan skannauksia vain tilaisuuden tullen tai tekemään myös pakollisia skannauksia, ja milloin pakolliset skannaukset suoritetaan. Sivulla kerrotaan myös niiden tukiasemien määrä, joissa on erillinen radio skannausta varten ja näyttää ne kartalla. Sivun alalaidassa näkyy lista havaituista uhista sekä niiden tila.

CMX:n keräämät ja analysoimat tiedot on esitetty Dashboardin sivulla Sijaintianalytiikka. Sivulla on yhteensä kuusi eri graafia, jotka ovat etäisyys, kaappausaste, sitoumus, vierailun keskipituus, lojaalius ja toistuvien vierailujen aste. Etäisyys kertoo verkossa liikkuneiden laitteiden määrän ja erittelee niistä ohikulkijat, vierailijat ja liittyneet käyttäjät. Sitoumus erittelee käyttäjien määrän vierailun pituuden mukaan ja vierailun keskipituus näyttää vierailujen keskimääräisen pituuden päivää kohden. Lojaalius erittelee käyttäjien määrän sen mukaan, kuinka usein he ovat vierailleet verkossa ja toistuvien vierailujen aste näyttää kaikista vierailijoista sen prosentuaalisen osuuden, jotka ovat vierailleet verkossa useammin kuin kerran. Lämpökartta (Location heatmap) esittää alueella olevien laitteiden määrän visuaalisesti. Kartta esittää laitteiden sijainnin tukiasemiin nähden ja näyttää laitteiden määrän eri väreillä. Esimerkiksi vihreällä alueella on vähiten laitteita punaisella eniten.

PCI-raportti (PCI report) on työkalu, jolla voidaan tarkistaa, onko jokin langattoman verkon asetukset PCI DSS -standardin mukaiset. Luotu raportti on hyvin yksityiskohtainen, ja se kertoo vaatimuskohtaisesti, täyttyvätkö standardin vaatimukset. Jos jokin vaatimus ei täyty, raportti kertoo, mitä ongelman korjaamiseksi tulisi tehdä ja ohjaa käyttäjän sille sivulle, mistä kyseisen asetuksen voi muuttaa. [27, luku 4.] Bluetooth käyttäjät-sivu (Bluetooth clients) on hyvin samanlainen sivu kuin Tukiasemat-sivu tai Käyttäjät-sivu, mutta sivu sisältää tiedot vain Bluetooth-käyttäjistä.

Radiotaajuusspektri-sivu (RF spectrum) näyttää reaaliaikaista spektrianalyysidataa niistä tukiasemista, joissa on WIPS-radio. Dataa voi käyttää vianhaussa tai sen avulla voi määrittää, millä taajuuskanavilla on eniten liikennettä. Sivu antaa ensin yleiskatsauksen tukiasemista, joissa spektrianalyysi on käytössä. Tukiasemista kerrotaan niiden käyttämät kanavat ja kanavien käyttöaste kummallakin taajuusalueella. Tukiasemien yksityiskohtaisissa tiedoissa taajuus kanavien käyttö on esitetty spektogrammeilla. Spektogrammi on graafinen esitys spektristä. Ylempi spektogrammi esittää käyttöasteen desibeleinä. Alemmassa spektogrammissa käyttöaste näytetään mitattujen näytteiden tilannekuvina sekunti sekunnilta. Tilannekuvien värit edustavat käyttöastetta (sininen, vihreä, keltainen, ja punainen). Spektrogrammien alla on vielä taulukko kaikista tukiasemalla käytetyistä kanavista, joka kertoo käyttöasteen prosentteina ja listaa muut tukiaseman läheisyydessä olevat tukiasemat, jotka saattavat aiheuttaa häiriöitä. [28.]

3.2 Verkon ja tukiasemien asetukset

Meraki-pilvessä on kahdenlaisia ylläpitäjiä, organisaation laajuisia ja yhden tai monen verkon laajuisia ylläpitäjiä, joille voi asettaa eri oikeuksia. Organisaatioylläpitäjällä voi olla täydet oikeudet tai lukuoikeudet organisaation tietoihin ja asetuksiin sekä kaikkiin organisaation verkkoihin. Lukuoikeudella tarkoitetaan perinteisesti lupaa tarkastella kaikkia organisaation tietoja, mutta ei lupaa muokata niitä. Yhden tai useamman verkon ylläpitäjällä voi olla Guest Ambassador-, valvonta-, luku-, tai täydet oikeudet. Guest Ambassador -oikeudet omaavalla ylläpitäjällä on pääsy vain Dashboardin käyttäjät-sivulle, josta hänellä on lupa lisätä käyttäjiä, päivittää nykyisten käyttäjien tietoja, ja antaa tai poistaa käyttäjän oikeudet liittyä verkkoon. Valvontaoikeuksilla pystyy katsomaan vain osaa valvonta osion sivuista ja verkkoon ei pysty tekemään muutoksia. Kaikkia organisaation ja verkkojen ylläpitäjiä voi hallita Organisation > Administrators -sivulta, mutta silloin täytyy

olla organisaation täydet oikeudet. Verkon ylläpitäjät voivat lisätä verkkoon uusia ylläpitäjiä ja muokata muiden ylläpitäjien oikeuksia. [29, luvut 1-4.]

Ylläpitäjä voi valita Access points > Access control -sivulta SSID-kohtaisesti, mitä salausta ja todennusta verkkoon liittyvien käyttäjien todennuksessa käytetään. Meraki tukee avointa todennusta, MAC-osoite todennusta, ennalta jaettuja avaimia ja WPA2-Enterprise:a, jossa on 802.1X-todennus. Avoin todennus sallii minkä tahansa laitteen liittymisen verkkoon. Vaihtoehto ei vaadi vaikeaa konfiguraatiota, ja sitä on hyvä käyttää, kun yhteyden saamisen on oltava helppoa ja silloin, kun verkkoon pääsyä ei tarvitse rajoittaa. Käyttäjä voidaan todentaa myös laitteen MAC-osoitteen perusteella RADIUS-serverin kautta. Tämä ei vaadi konfigurointia asiakkaan puolelta, mutta Access control -sivulla täytyy olla konfiguroituna vähintään yksi RADIUS-serveri. Verkko voidaan suojata ennalta jaetulla avaimella (PSK, pre-shared key) eli salasanalla, jonka yhteydessä käytetään WEP-, WPA- ja/tai WPA2-todennusta. Access control -sivulta voi valita, käytetäänkö WEP- vai WPA-todennusta. Jos WPA valitaan, voidaan vielä määrittää, käytetäänkö pelkästään WPA2:sta vai alkuperäistä WPA:ta ja WPA2:sta yhdessä. WEP ja WPA ovat nykyään haavoittuvaisia protokollia, joten WPA2:den käyttö on suositeltavaa, mutta samalla WPA2 ja edes WPA eivät ole aina yhteensopivia vanhempien laitteiden kanssa. WPA2-Enterprise toimii yhdessä IEEE 802.1X-standardin kanssa, joka on salaus- ja todennusviitekehys. 802.1X käyttää AES-salausta ja EAP-protokollaa, joka luo turvatun yhteyden todennusprosessia varten. WPA2-Enterprise hakee käyttäjän tiedot todennusta varten joko Merakin ylläpitämästä todennuspalvelimesta tai yrityksen omalta RADIUS-serveriltä. Silloin kun Merakin ylläpitämä todennus on käytössä, ylläpito lisää käyttäjien tiedot Network wide > Users -sivulta. [30.]

Splash-sivu, tai captive portal, on ikkuna, joka avautuu asiakkaalle ennen kuin hän pystyy jatkamaan haluamallensa internetsivulle, tai Merakin tapauksessa silloin, kun selain avataan ensimmäisen kerran ja ensimmäinen HTTP-pyyntö on lähetetty. Sivun tarkoitus on saada käyttäjä huomioimaan sivun sisältö ennen kuin hän voi jatkaa. Splash -sivu voi olla pelkästään click-through-sivu tai kirjautumissivu. Kirjautumisen voi määrittää maksulliseksi, joko kortilla tai tekstiviestillä, ja sen voi määrittää toimimaan myös Facebook tai Google -tunnuksilla. Ylläpidon tulee huomioida, että kaikki laitteet, kuten langattomat viivakoodin lukijat, eivät pysty käyttämään selainta, milloin nämä laitteet eivät voi liittyä verkkoon, ellei sitä ole erikseen asetuksissa sallittu. Click-through-sivulta pääsee eteenpäin ”jatka” -painiketta klikkaamalla. Sivu on täysin muokattava HTML-sivu, jonka yritys voi tehdä sen näköiseksi kuin itse haluaa. Sivulla voi olla esimerkiksi yrityksen väriteema

ja logo, tai sillä voidaan esittää yrityksen palveluehdot. Click-through-sivu on aina Merakin ylläpitämä, minkä vuoksi yhteyden pilveen on toimittava, jotta myös click-through-sivu toimii. [31.]

Kirjautumissivu on click-through-sivun tavoin täysin muokattavissa, mutta jatkaakseen asiakkaan täytyy syöttää sivulle käyttäjätunnus ja salasana, jotka on määritelty joko Merakin-, RADIUS-, Active Directory-, tai LDAP-serverille. Todennus on suojattu SLL:llä (HTTPS) ja käyttäjän täytyy uudelleenkirjautua tietyin väliajoin [31, luku 2]. Splash-sivu voidaan määrittää käyttämään pääsyehtona laskutusta, eli asiakas suorittaa yritykselle maksun luottokortilla tai prepaid-kortilla. Luottokorttimaksu toteutetaan yhdessä ulkopuolisen palveluntarjoajan kanssa. Merakin kanssa toimivat tarjoajat ovat Splash Access, Cloud4Wi, Purple WiFi ja SOCFI. Palveluntarjoaja käsittelee laskutustapahtuman, mikä tarkoittaa, että ylläpidon ei tarvitse huolehtia luottokorttimaksun yhdyskäytävän konfiguroimisesta ja ylläpidosta. [31, luku 4.1.] Prepaid-kortit ovat pääsykoodeja, jotka ylläpito voi luoda erissä. Erilaisia laskutussuunnitelmia voi olla samanaikaisesti viisi ja ne voidaan määritellä niin, että verkkoa voi käyttää tietyn ajanjakson ajan määrätyllä nopeudella tiettyä summaa vastaan (esimerkiksi 5 €/kk 1 megabitin nopeudella). Prepaid-vaihtoehdon yhteydessä voi myös määrittää tietyn mittaisen vapaan pääsyn verkkoon, esimerkiksi niin sanotuksi kokeiluajaksi ennen kuin asiakkaalta peritään maksu. [31, luku 4.2.] Kirjautumiseen voidaan käyttää myös tekstiviestiä, joka on myös yksi laskutuksen muoto (lähtevän viestin hinta). Käyttäjä saa paluuviestinä koodin, jolla hän voi kirjautua verkkoon. Jokainen Merakin verkko tarjoaa aluksi 25 ilmaista kirjautumista, mutta sen jälkeen ylläpidon täytyy luoda tili Twilio-nimiseen palveluun, joka hoitaa laskutuksen tästä eteenpäin. Twilio-tilin tiedot lisätään Network wide > General –sivulle. [31, luku 5.]

Facebook-tunnuksilla kirjautuminen on tapa liittää verkkoon kirjautuminen sosiaaliseen mediaan. Yritys voi käyttää omaa Facebook-sivuaan kirjautumissivuna, joka tuo yrityksen sivuille näkyvyyttä ja antaa mahdollisuuden tuoda tarjouksia ja ilmoituksia asiakkaille. Google-tunnuksilla kirjautuminen yksinkertaisesti ohjaa uuden käyttäjän splash-sivulle, jossa hänelle annetaan vaihtoehto kirjautua verkkoon omilla Google-tunnuksillaan. [31, luku 6;32.] Kaikki splash-asetukset määritellään Wireless > Access Control -sivulta ja niiden splash-sivujen, joiden ulkoasua voi muokata, ulkoasu-asetukset määritellään Wireless > Splash -sivulta. Kaikkien erilaisten splash-sivujen kohdalla voi määrittää seuraavat asetukset:

- Network Access Control (NAC): vain laitteet, joissa on Merakin tukema virustorjuntaohjelma, voivat liittyä verkkoon [33].
- Group policy: eri laitteille määritetyt ryhmäkäytännöt ovat käytössä automaattisesti.
- Salli tai estä muu kuin HTTP-liikenne ennen kirjautumista.
- Wallen Garden: Määritä IP-osoitealue, jolle käyttäjällä on pääsy ennen kirjautumista.
- Salli uusien käyttäjien luoda omat tunnukset (ylläpidon täytyy hyväksyä luodut tunnukset ennen kuin ne astuvat voimaan).
- Salli kirjautuminen samanaikaisesti usealla laitteella.
- Määritä verkon toiminta yhteyden tai Merakin pilven ollessa alhaalla: avoin, rajattu tai oletusarvo.

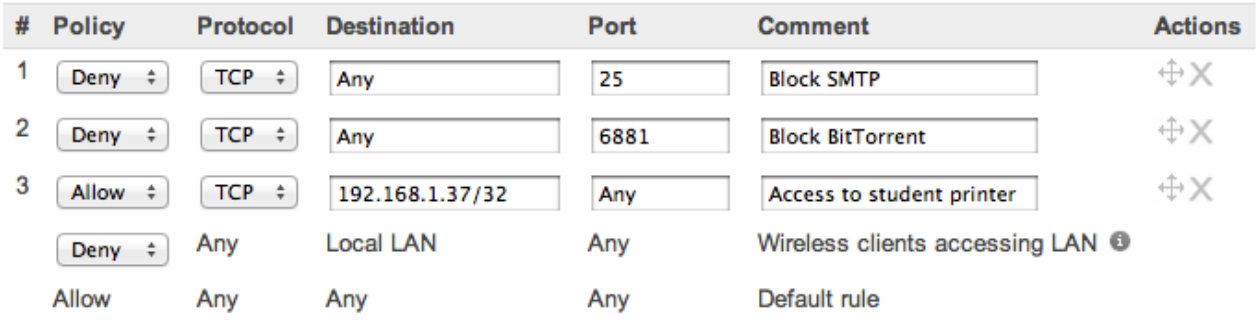
RADIUS-, LDAP- ja Active Directory-servereiden kohdalla täytyy määrittää myös käytettävän serverin tiedot. Jos yritys haluaa käyttää Google-tunnuksilla kirjautumista, ”Sign-on with” -kohdassa valitaan ”3rd party credentials”, jonka jälkeen aukeavaan ”Accepted credentials” -kohtaan valitaan Google. Tämän lisäksi aukeaa ”Allowed domains” -kohta, mihin täytyy määrittää Googlen domain, jos muu kuin HTTP-liikenne ei ole sallittu ennen kirjautumista, koska muuten selain ei voi avata kirjautumisikkunaakaan [34]. Facebook-tunnuksien kohdalla valitaan ”Facebook WiFi” -vaihtoehto. Kun ylläpitäjä tallentaa tekemänsä muutokset, Dashboard ohjaa ylläpitäjän sivulle, josta hän voi konfiguroida Facebook WiFi:n asetukset [32]. Merakin tarjoamien vaihtoehtojen lisäksi yritys voi myös liittää Merakiin myös ulkoisen splash-sivun.

Access control -sivulta määritetään tapa, jolla IP-osoitteet jaetaan eri verkojen sisällä. Tukiasemien kanssa käytettävät vaihtoehdot ovat Network Address Translation -tila (NAT), Bridge-tila, ja Layer 3 roaming. NAT-tilassa tukiasema toimii DHCP-serverinä ja jakaa asiakkaille NAT:in sisältä IP-osoitteen yksityisestä 10.x.x.x-osoitealueesta. NAT-tilaa tulee käyttää seuraavissa tapauksissa:

- Asiakkaat tarvitsevat vain internet-yhteyden, mutta eivät pääsyä lankaverkon tai langattoman verkon resursseihin.
- Lankaverkossa ei ole DHCP-serveriä, joka voisi jakaa osoitteita langattomille asiakkaille.
- Lankaverkossa on DHCP-serveri, mutta sille annettu osoitealue ei ole riittävän suuri jakamaan osoitteita myös langattomille asiakkaille. [35, luku 2.]

Bridge-tilassa tukiasema toimii siltana, jonka kautta DHCP:ltä annetut osoitteet jaetaan käyttäjille. Bridge-tilan käyttö sopii silloin, kun verkko ei vaadi NAT-tilan käyttöä. [35, luku 1.] Layer 3 roaming säilyttää laitteen IP-osoitteen, vaikka sen sijainti muuttuisi niin, että laite ei enää saa yhteyttä siihen tukiasemaan ja VLAN:iin, johon se alun perin yhdistyi. Layer 3 roaming on hyödyllinen silloin, kun on tärkeää, että langattoman laitteen yhteys verkkoon ei katkeile, kuten VoIP-sovellusta käytettäessä. [35, luvut 3-4.] NAT-tilan yhteydessä on mahdollista ottaa käyttöön sisällön suodatus, jolla voidaan estää käyttäjien pääsy aikuisviihdesivustoille. Suodattimen voi määrittää käyttämään Merakin omaa listaa yleisistä aikuisviihdesivustoista tai mukautettua DNS-palvelinta. Mukautettu DNS-palvelin ohjaa liikenteen tavallisesti käytettävältä palvelimelta Dashboardiin määritetylle palvelimelle, jossa on mukautettu lista suodatettavista sivuista. [36.]

Merakin tarjoamien turvaominaisuuksien lisäksi Dashboardista löytyy mahdollisuus luoda palomuurisääntöjä Wireless > Firewall & traffic shaping -sivulta. Rajoittamalla, tai sallimalla, tiettyä liikennettä tai sovelluksia, ylläpito voi hallita verkon suojausta sekä liikenteen määrää erittäin yksityiskohtaisesti. Palomuurisäännöillä voi taata tiettyjen käyttäjien pääsyn vain heille suunnattuihin resursseihin. Ne ovat erittäin hyödyllisiä silloin, kun verkossa on käytössä avoin todennus. Säännöt voi lisätä SSID-kohtaisesti tai ne voi liittää ryhmäkäytäntöihin. Liikennettä muokkaavat säännöt koskevat OSI-mallin verkkokerrosta, eli kerrosta numero kolme, ja niitä kutsutaan Dashboardissa nimellä ”Layer 3 firewall rules”. Sovelluksien käyttöä muokkaavat säännöt koskevat sovelluskerrosta, eli kerrosta numero seitsemän, ja niitä kutsutaan Dashboardissa nimellä ”Layer 7 firewall rules”. Liikennettä koskevat säännöt voivat olla seuraavanlaisia:



Kuva 2. Esimerkkejä erilaisista Layer 3 -palomuurisäännöistä. [37.]

Policy-kohdasta valitaan, sallitaanko liikenne vai ei. Protocol-kohdasta valitaan protokolla, jota sääntö koskee. Destination-kohtaan voidaan määrittää jokin tietty kohde, mitä sääntö koskee. Port-kohtaan voidaan määrittä portti, josta liikenteen lähtö sallitaan tai kielletään, ja comment-kohtaan voi kirjoittaa muistiin säännön tarkoituksen. Sovelluksia koskevat säännöt on luotu niin, että IP-osoitteita tai portteja ei tarvitse määrittää, vaan sääntö määritetään koskemaan joko yksittäistä sovellusta tai kokonaista sovelluskategoriaa, kuten kaikkia musiikki- videosivustoja. Layer 7 palomuurisäännöissä policy on aina ”deny”, ja application-kohdasta valitaan se sovelluskategoria, joka halutaan estää, ja vielä halutessa yksi tietty sovellus, joka halutaan estää. [37.] Firewall & traffic shaping -sivulta voi myös rajoittaa SSID:n ja käyttäjien käyttämää kaistanleveyttä. Kaistanleveyttä voi rajoittaa yleisesti käyttäjäkohtaisesti ja SSID-kohtaisesti käyttäjän ja verkon suuntaan. Merakista löytyy speed burst -ominaisuus, joka antaa käyttäjän ylittää hänelle asetetun kaistanleveyden tarvittaessa.

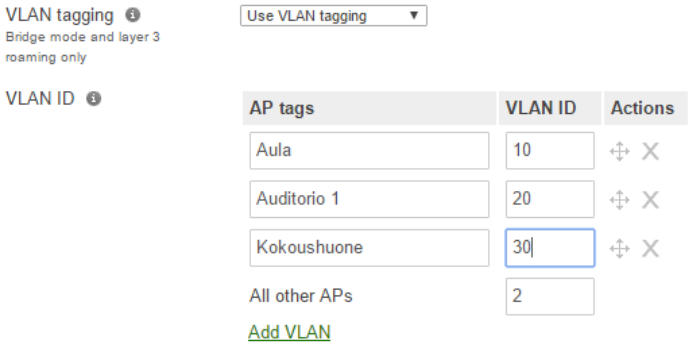
Yleisten rajoitusten lisäksi sivulla voi luoda sääntöjä, joilla voi rajoittaa tiettyihin sovelluksiin ja sivuihin käytettävää kaistanleveyttä. Tämä mahdollistaa ei-toivotun liikenteen kaistanmäärän pienentämistä samalla, kun tärkeäksi luokiteltu liikenne käsitellään normaalisti. Definition-kohtaan valitaan se tai ne sivustot tai sovellukset, joihin käytettävän kaistan kokoa halutaan rajoittaa. Jos haluttua vaihtoehtoa ei löydy valmiista luettelosta, ylläpito voi luoda oman kohteen käyttämällä isäntänimeä, IP-osoitetta, kohdeporttia tai lähdeverkon osoitetta. Asiakaskohtaiseen kaistanmäärään valitaan ylin sallittu kaistaleveys asiakkaan suuntaan ja asiakkaalta verkkoon. Näiden sääntöjen yhteyteen on liitetty mahdollisuus muuttaa tietyn liikenteen QoS-prioriteettia. Meraki tukiasemat tukevat Wireless Multimedia Extensions -protokollaa (WMM), joka huolehtii liikenteen laadusta PCP- ja DSCP-merkintöjen avulla. PCP-merkintä, eli Priority Code Point, lisätään IEEE 802.1q-standardin otsikkokehykseen kaikessa tukiasemalta käyttäjälle kulkevassa liikenteessä. PCP-merkintä on kuitenkin käytössä vain VLAN tagging -ominaisuuden kanssa. DSCP-merkintä, eli Differentiated Services Code Point, lisätään kaikkien lähtevien ja saapuvien IP-pakettien otsikkokehykseen. Merkinnöillä voidaan priorisoida esimerkiksi VoIP-liikenne, joka vaatii korkean prioriteetin, että puhelu ei katkeilisi, samalla kun vain dataa siirtäville käyttäjille annetaan alempi prioriteetti. [38.]

Kuten perinteisissäkin verkoissa, Merakin tukiasemilla voi luoda VLAN-verkkoja (Virtual Local Area Network). VLAN-verkon tarkoitus on ryhmitellä käyttäjiä niin, että yksi fyysinen verkko näkyy monena loogisena verkkona. Tätä asetelmaa voi käyttää verkon suojauksen parantamiseen, avoimen todennuksen tueksi, tai broadcast-viestien rajoittamiseen. Merakin tapa luoda VLAN:it on IEEE 802.1Q-standardin VLAN tagging. VLAN luodaan merkitsemällä haluttu liikenne valitulla tunnisteella (VLAN ID). Kun merkitty liikenne kulkee tukiasemalta kytkimeen tai reitittimeen, saman merkinnän omaava liikenne tunnistetaan tiettyyn VLAN:iin kuuluvaksi liikenteeksi ja siihen voidaan automaattisesti liittää ennalta määrättyjä sääntöjä tai käytäntöjä (palomuuri tai esimerkiksi QoS-käytäntö VoIP-liikennettä varten). Vastavuoroisesti, kun tukiasema vastaanottaa merkittyä liikennettä, se osaa ohjata liikenteen oikealle SSID:lle tai käyttäjälle ja tiputtaa liikenteen, jolla on VLAN ID, joka ei ole tukiaseman tai sen käyttäjien käytössä. [39.] VLAN tagging on käytössä vain bridge-tilassa ja yhdyskäytävänä toimiva tukiasema tulee liittää muuhun verkkoon sellaiseen kytkimen tai reitittimen porttiin, joka on konfiguroitu trunk-portiksi. Merakista pilveen suunnattu hallinta-liikenne kulkee verkossa ilman VLAN ID:tä. Trunk-portti liittää tällaisen merkitsemättömän liikenteen poikkeuksetta natiivi VLAN:iin, minkä takia on tärkeää, että kaikilla verkon laitteilla on sama natiivi VLAN. VLAN tagging vaatii toimiakseen seuraavat asetukset:

- Kaikilla tukiasemilla täytyy olla IP-osoite samasta aliverkosta natiivi VLAN:in kanssa staattisesti tai DHCP:n kautta.
- Portti, johon tukiasema liitetään, tulisi konfiguroida 802.1Q trunk-portiksi ja tämän portin kapsulointi tulisi olla 802.q trunk encapsulation.
- Trunk-portti tulisi konfiguroida sallimaan kaikki jokaiselle SSID:lle luodut VLAN:it ja jokaisella SSID:llä tulisi olla ainakin yksi VLAN, joka on konfiguroitu paikalliseen lankaverkkoon.
- Merakin hallinta-liikenteellä täytyy olla pääsy internettiin, eli Merakin pilveen, ja serveriin autentikointia varten. [40.]

VLAN tagging voidaan toteuttaa SSID-kohtaisesti, käyttäjäkohtaisesti, laite-kohtaisesti, tai tukiasema-kohtaisesti. Koko SSID:lle voi tehdä vain yhden VLAN:in tai useamman, jos yhden SSID:n sisällä kulkevaa liikennettä haluaa ryhmitellä. [39.] VLAN tagging otetaan käyttöön Wireless > Access control -sivulta Addressing and traffic -osiosta ja VLAN:it määritellään ”VLAN ID” -kohtaan. Silloin kun verkossa halutaan käyttää yhtä VLAN:ia, se lisätään VLAN listasta jo valmiiksi löytyvään kohtaan ”All other AP’s”, joka

merkitsee kaikkea tämän verkon kautta kulkevaa käyttäjä-liikennettä tukiasemasta riippumatta. Jos liikenne halutaan ryhmitellä eri VLAN:eihin tukiasema-kohtaisesti, tukiasemalle pitää ensin luoda tunniste Wireless > Access points -sivulla, joka sitten lisätään VLAN ID listaan ja jolle määritetään oma VLAN-tunniste. [40.]



Kuva 3. VLAN:ien määrittely Dashboardissa

Kun VLAN ID konfiguroidaan käyttäjäkohtaisesti, monet käyttäjät voivat olla yhdistyneenä samaan verkkoon, mutta eri käyttäjiltä lähtevällä liikenteellä voi olla eri tunnisteet. Yleisesti tämä on toteutettu RADIUS-serverin avulla MAC-pohjaisen todennuksen tai WPA2-Enterprise-todennuksen kanssa niin, että kun käyttäjä todennetaan, serveri lähettää käyttäjälle viestin, josta ilmenee se VLAN ID, joka kuuluu kyseiselle käyttäjälle. Jos käyttäjä liitetään todennuksen yhteydessä tiettyyn ryhmäkäytäntöön, ja tämä käytäntö sisältää tunnisteen, niin tämä tunniste annetaan käyttäjälle. VLAN-tunnisteen sisältävän käytännön voi asettaa käyttäjälle myös manuaalisesti. Laitekohtainen VLAN tagging toimii yhdessä laitekohtaisten ryhmäkäytäntöjen kanssa. Kun Meraki tunnistaa verkkoon liittyvän laitteen tyypin tai mallin ja liittää siihen automaattisesti näitä laitteita varten luodun käytännön, laite saa tämän käytännön kautta automaattisesti myös VLAN-tunnisteen, jos sellainen on kyseiseen käytäntöön määritelty. [39.]

VLAN tagging:in yhteydessä voi ottaa käyttöön Bonjour-protokollan. Bonjour on Applen kehittämä Zero Configuration -protokollaan perustuva tekniikka, jonka avulla verkossa olevat päätelaitteet voivat löytää toisensa ja keskustella keskenään automaattisesti ilman konfigurointia. Bonjour toimii monissa muunkin valmistajan laitteissa, koska Zero Configuration on niin laajalti hyödynnetty protokolla. [41.] Bonjourin avulla esimerkiksi tulostin voidaan liittää verkkoon niin, että sen IP-osoitetta ei tarvitse syöttää verkon jokaiseen päätelaitteeseen, vaan päätteet pystyvät havaitsemaan tulostimen ja selvittämään sen IP-osoitteen automaattisesti. Toisaalta sovellukset voivat havaita toisiaan ja

jakaa keskenään esimerkiksi musiikkia tai valokuvia. [42.] Laitteet ja sovellukset mainostavat itseään toisilleen Multicast DNS -protokollan avulla (mDNS) [43]. Multicast DNS (mDNS) mahdollistaa perinteiset DNS-palvelin toiminnot silloin, kun verkosta ei löydy DNS-palvelimena toimivaa serveriä. Protokolla vapauttaa myös osan DNS-nimiavaruudesta paikalliseen käyttöön, joka sallii sen, että käyttäjän laitteelle antamaa nimeä voidaan käyttää osana DNS-isäntänimeä [44, Abstract]. Tämä mahdollistaa laitteiden yksilöinnin mDNS-viesteissä silloin kun laitteet kommunikoivat keskenään [44, luku 3].

Yksi Bonjourin rajoite on, että kaikkien keskenään yhteydessä olevien laitteiden täytyy olla samassa aliverkossa. Meraki on ratkaissut ongelman Bonjour forwarding ominaisuudella, jonka avulla Bonjour-laitteet voivat keskustella usean VLAN:in yli ohjaamalla kaiken Bonjour-liikenteen yhdelle palvelu-VLAN:ille. Liikenteen ohjaus määritellään luomalla sääntöjä, joista käy ilmi, minkä palvelun tai palveluiden liikenne ohjataan millekin VLAN:ille, eli kaikille palveluille voidaan luoda yksi yhteinen VLAN tai vaihtoehtoisesti palvelut voidaan ohjata usealle eri VLAN:ille. Bonjour forwarding toimii vain bridge-tilassa, koska se sallii verkon laitteiden keskinäisen kommunikoinnin. Jos ping-komennot eivät kulje laitteiden välillä, Bonjour ei voi toimia. Bonjour otetaan käyttöön Dashboardin Access control -sivulta Addressing and traffic -osiosta. [45.]

Access control -sivun wireless options -osiosta voi hallita taajuuskanavien käyttöä ja sallittuja bittinopeuksia. Osiosta voi määrittää tukiaseman käyttämään molempia taajuuskanavia samanaikaisesti tai vain 5 GHz:n kanavaa. Meraki tarjoaa näiden lisäksi kolmannen ”Band steering” -vaihtoehdon, jonka avulla voidaan määrätä kummaan kanavan kautta laitteet ottavat yhteyden verkkoon, perustuen siihen, pystyykö laite käyttämään 5 GHz:n taajuusaluetta. Band steering ohjaa ne laitteet, jotka kykenevät käyttämään 5 GHz:n aluetta tälle kanavalle, mikä vähentää laitteiden määrää ja lisää kaistaa usein ruuhkautuneella 2,4 GHz:n alueella. Band steering perustuu langattomien laitteiden tapaan löytää WLAN-verkkoja. Langaton laite suorittaa passiivisia ja aktiivisia skannauksia havaitakseen tukiasemien mainostamia verkkoja. Passiivisessa skannauksessa laite tutkii taajuuskanavat nopeasti havaitakseen verkkoja. Aktiivisessa skannauksessa laite lähettää niille tukiasemille, joilta se on havainnut verkon, pyynnön, jossa se pyytää tukiasemaa tarkistamaan, onko tukiaseman mainostama verkko yhteensopiva laitteen kanssa. Yhteensopivuuteen vaikuttaa esimerkiksi tuettu datan siirtonopeus ja käytetty salaustyyppi. Jos sopiva verkko löytyy, tukiasema vastaa pyyntöön ilmoittamalla laitteelle sopivasta verkosta. Käytännössä tämä vastaus näkyy käyttäjälle laitteen antamana listana niistä verkoista, joihin käyttäjä voi liittyä.

Kun band steering on käytössä, tukiasema mainostaa verkkoja vain aktiivisen skannauksen tapahtuessa, minkä takia passiivisessa skannauksessa havaitut verkot luetellaan piilotetuiksi. Ylläpidon tulee huomioida, että laitteet, jotka käyttävät vain passiivista skannausta akun varauksen säästämiseksi, eivät välttämättä kykene löytämään verkkoa ollenkaan, kun kanavan ohjaus on käytössä. Jos tukiasema vastaanottaa aktiivista skannausta suorittavalta laitteelta tiedustelupyynnön molemmilta kanavilta lyhyen ajan sisällä, tukiasema mainostaa verkkoa vastauksena vain 5 GHz:n kanavalta tulleeseen pyyntöön, koska se havaitsee laitteen kykenevän käyttämään tätä taajuusaluetta. Näin kaikki laitteet, jotka kykenevät käyttämään 5 GHz:n taajuusaluetta voidaan ohjata tälle kanavalle, ja ne laitteet, joilta ei vastaanoteta tiedustelupyyntöä 5 GHz:n kanavalta, ohjataan automaattisesti 2,4 GHz:n kanavalle. [46.] Alhaisten bittinopeuksien estämisen voi vapauttaa langattoman verkon kaistaa, sillä se lyhentää aikaa, jonka hitaammat laitteet voivat käyttää datan lähettämiseen verkossa. Pienimmän sallitun bittinopeuden asettaminen liian korkeaksi saattaa kuitenkin kokonaan estää 802.11b-standardia käyttävien laitteiden liittymisen verkkoon. [47.]

Network wide > General -sivulta voi hallita määritettyjen verkkojen ylläpitäjiä ja muuttaa tukiaseman yleiseen toimintaan liittyviä asetuksia. Traffic analysis -osiosta voi muuttaa seuraavia käytäntöjä: poistaa käytöstä liikenteen valvonnan ja verkossa vierailevien laitteiden tietojen, kuten isäntänimet ja IP-osoitteet, tarkan raportoinnin. Tästä kohdasta voi myös muokata luvussa 3.1 mainittua ympyrädiagrammia lisäämällä siihen omia osioita. CMX -osiosta voi valita halutaanko verkossa käyttää CMX-analytiikkaa ja käytetäänkö sen kanssa myös CMX API:a (luku 3.3). Packet capture -osiosta voi määrittää Merakin ohjaamaan tukiaseman suorittamat pakettien kaappaukset analysoitavaksi kolmannen osapuolen CloudShark -analysointiohjelmaan, joka on toiminnaltaan hyvin samanlainen kuin ehkä käyttäjille tutumpi WireShark. Device configuration -osiosta voi muuttaa seuraavia tukiaseman asetuksia:

- Poistaa käytöstä tukiaseman lokaalin hallintasivun (My Meraki, luku 4.2).
- Määrittää salasanan, jota tarvitaan kirjautuessa lokaalille tilasivulle.
- Sallia laitteen tarkastelun etäyhteydellä laitteen LAN IP-osoitteen avulla.
- Määrittää miten niiden käyttäjien, jotka ovat liittyneet johdolla suoraan tukiasemaan, kohdalla toimitaan. Käyttäjien pääsyn voi kieltää tai käskeä tukiasemaa käyttämään samoja asetuksia kuin normaalia verkkoon liittyvää käyttäjää.

- Antaa tukiasemalle staattisen IP-osoitteen.
- Kieltää IPv6-liikenne. Jos IPv6-liikenne sallitaan, verkon täytyy olla Bridge-tilassa.
- Kytkeä tukiaseman fyysiset LED-valot pois päältä.

Network alerts -osiosta voi valita, mistä verkon ja tukiaseman tapahtumista lähetetään ilmoitus ylläpidolle ja mihin sähköpostiosoitteeseen tai -osoitteisiin ilmoitus lähetetään. SNMP-osiosta voi sallia Simple Network Management Protokollan käytön ja valita, mitä versiota protokollasta käytetään. SNMP on protokolla, jonka avulla voidaan tiedustella erinäisiä laitetietoja. Kun yhteys muodostetaan versioiden yksi tai kaksi kanssa, siihen täytyy käyttää osioon määritettävää yhteisönimeä. Version kolme kanssa käytetään käyttäjätilejä (käyttäjänimi ja salasana), jotka voi myöskin määritellä tähän osioon. [48.]

RTLS-osiosta voi ottaa käyttöön Ekahaun tai Stanleyn (ent. AeroScout) kehittämän RTLS-järjestelmän. RTLS, eli Real Time Location Services, on laitteiden sijainnin jäljittämistä varten kehitetty sovellus. [49.] Firmware upgrade -osiosta voi määrittää, milloin laitteet päivitetään ja sallitaanko laitteissa beta-testauksessa olevien ominaisuuksien käyttö. Public network status page -osiosta voi ottaa käyttöön kaikille julkisen verkonlaajuisen tilasivun. Sivulta käy ilmi esimerkiksi tukiasemien sijainti ja tila, käyttäjien määrä ja siirretyn datan määrä. Internetsivun lisäksi tiedot ovat saatavissa XML- tai KML-syötteenä. XML-syöte näyttää tiedot Microsoft Excel formaatissa, joka on helppo tapa jäsentää tukiasemista saatua tietoa. KML, eli Keyhole Markup Language, on eräänlainen XML-tiedosto, joka sisältää tiedot tukiasemien sijainneista. Maantieteellisiä sijainteja voi tarkastella Google Earth -selaimella [50;51].

Tilasivun voi myös ottaa käyttöön niin, että laitteiden koordinaatit on piilotettu. XML-syötteessä tämä tarkoittaa sitä, että sijaintia ei ilmoiteta, mutta KML-syötettä ei voida luoda, jos koordinaatit on piilotettu. Selaimessa näkyvä tilasivu näyttää laitteiden tiedot samalla Google Maps kartalla, joka löytyy Dashboardista. Kartalla näkyy myös pohjapiirustukset, jos niitä on lisätty Dashboardiin. Kartalla näkyviltä tukiasemista voi aikaisemmin mainittujen tietojen lisäksi nähdä myös tukiaseman mallin, nykyisten käyttäjien määrän, käyttäjien määrän viimeisen 24 tunnin aikana ja kuinka monen hypyn päässä yhdyskäytävä

on. Kartalla voidaan näyttää myös mesh-naapureiden väliset linkit, ja jokaisen tukiaseman käyttöaste voidaan esittää ympyränä laitteen sijainnin kohdalla (isompi ympyrä = isompi käyttöaste). [51.]

SSID availability -sivulta voi määrittää, mitkä SSID:t ovat käytössä milläkin tukiasemalla ja lisäksi, mihin aikaan päivästä mikäkin SSID on käytössä. Sivulta valitaan SSID-kohtaisesti, mainostetaanko verkkoa julkisesti, mainostetaanko verkkoa kaikilla tukiasemilla vai vain tietyllä merkinnällä tai tietyillä merkinnöillä merkatuilla tukiasemilla, ja milloin verkkoa mainostetaan. Verkkoa voi halutessa mainostaa joka päivä eri kellonaikaan. [52.] Bluetooth settings -sivulta voi ottaa käyttöön bluetooth-ominaisuuksien mainostuksen. Kun mainostus on käytössä, tukiasemiin integroitu Bluetooth Low Energy -radio (BLE) lähettää tasaisin väliajoin signaaleja, joita esimerkiksi älypuhelimet voivat vastaanottaa ja joihin älypuhelimessa oleva sovellus voi vastata. Bluetooth-radiolle annetaan yksilöllinen tunniste (Universally Unique Identifier, UUID), jonka voi generoida ko. sivulta, eli sitä ei tarvitse keksiä itse. Radiolle voi myös määrittää major- ja minor-tunnisteet (numero), jotka kuvaavat radion tai radioiden sijaintia. Major kuvaa yleensä kaikkia radioita yhden alueen sisällä, esimerkiksi toimistorakennus, ja minor kuvaa yksittäistä radiota tämän alueen sisällä. Lisäksi sivulta voi ottaa käyttöön BLE-skannauksen, jossa radio havaitsee lähistöllä olevia Bluetooth-laitteita ja tallentaa niiden tiedot wireless > Bluetooth clients -sivulle. [53.]

Radio settings -sivulta voi muuttaa tukiasemien radioiden asetuksia koko verkon osalta ja tukiasemakohtaisesti. Sivulta voi vaihtaa radioiden tehoa, ottaa Dynamic Frequency Selection -ominaisuuden (DFS) pois käytöstä, ja valita 5 GHz:n taajuusalueella oletuksena käytettävän kanavan leveyden. Jokaisen tukiaseman osalta voi määrittää erikseen 5 GHz:n alueella käytettävän kanavan leveyden, ja molemmille taajuusalueille käytettävän taajuuskanavan sekä tehon. Jokaisen näistä voi myös asettaa automaatti-tilaan, milloin tukiasema valitsee sopivat asetukset itse. Group policies -sivulta voi määrittää erilaisia sääntöjä, rajoituksia, ja muita asetuksia, jotka vaikuttavat siihen, miten tukiasema toimii eri käyttäjien kohdalla. Meraki-tukiasemat tarjoavat kahdeksan eri asetusvaihtoehtoa käytäntöjen luomiseen:

- Sheduling: käytännöt voivat olla käytössä määritettyinä päivinä ja kellonaikoina.
- Per-client bandwidth limit: käyttäjäkohtaista kaistanleveyttä voidaan rajoittaa.

- Hostname visivility: Käyttäjätietojen, kuten isäntänimi ja IP-osoite, tarkka raportointi voidaan ottaa pois käytöstä.
- VLAN tag: Sallii VLAN tagging -ominaisuuden käytön, tai käyttää aktiivisen SSID:n määrityksiä.
- Splash page authorization: Sallii käyttäjien ohittaa aktiivisen SSID:n splash-sivun, tai käyttää aktiivisen SSID:n määrityksiä.
- Layer 3 & Layer 7 firewall rules: Käytäntöön voi luoda erikseen omat palomuurisäännöt, käyttää aktiivisen SSID:n sääntöjä, tai jättää ne kokonaan pois käytöstä.
- Traffic shaping rules: Jos palomuurisäännöt-ominaisuus on käytössä, käytäntöön voi myös luoda käyttäjien kaistanleveyttä rajoittavia sääntöjä, tai käyttää aktiivisen SSID:n sääntöjä.

Meraki-tukiasemissa ryhmäkäytäntöjä voi asettaa käyttäjälle käyttäjäkohtaisesti, laitekohtaisesti ja RADIUS-serverin kautta. Käyttäjäkohtaiset käytännöt voidaan asettaa käyttäjille manuaalisesti network wide > clients-sivulta ja käyttäjälle voi myös asettaa eri käytäntöjä sen perusteella, mihin SSID:hen käyttäjä liittyy. Laitekohtaiset käytännöt asetetaan wireless > access control -sivulta network access -osiosta. [54.] RADIS-serverin kautta voi asettaa käytäntöjä, kun WPA2-Enterprise todennus on käytössä RADIUS-serverin kanssa. RADIUS-serverin asetuksiin pitää määrittää, mikä todennuksen yhteydessä lähetettävä viestiosio sisältää tiedon käyttäjälle asetettavasta käytännöstä, ja tieto tästä viestiosiosta lisätään Dashboardiin määritettyihin RADIUS-serverin tietoihin. [55.] Users-sivulta voi luoda SSD-kohtaisia käyttäjätilejä manuaalisesti. General-sivulla luodut ylläpitäjät näkyvät listalla automaattisesti, mutta näille käyttäjille ei anneta valtuuksia automaattisesti, vaan ne täytyy antaa manuaalisesti. Tavallisten käyttäjien valtuudet määritetään tilin luonnin yhteydessä. [56.]

3.3 Tukiasemien lokaali hallinta

My.meraki.com on Ciscon kehittämä etäyhteyspalvelu tukiaseman hallintaa varten. Käyttäjä kirjautuu sisään etäyhteys palveluun automaattisesti, jos tietokone on yhteydessä siihen tukiasemaan, jota halutaan tarkastella. Muussa tapauksessa sivusto pyytää käyttäjää kirjautumaan sisään tukiaseman sarjanumeroa käyttäen.

Palvelun aloitussivu on Connection-välilehti. Tältä sivulta voi tarkistaa käyttäjä-tietokoneen tiedot (IP-osoite, MAC-osoite, käytössä oleva tukiasema radio ja taajuuskanava,

käytetty 802.11x-standardi, maksimaalinen bittinopeus ja signaalin voimakkuus) sekä itse tukiaseman tiedot (laitteen ja verkon nimi, fyysinen MAC-osoite, laitteen mallinumero tai nimi, käytettävissä olevien taajuuskanavien käyttöaste, Ethernet-yhteyden tiedot, Internet-yhteyden tila ja Meraki pilvi-yhteyden tila). Sivulta löytyy myös selainpohjainen yhteyden nopeustesti. Neighbors-välilehti näyttää jokaisen muun havaitun yhteyden ja jakaa ne kahteen ryhmään sillä perusteella, onko kyseessä toinen Meraki laite vai jokin muu yhteys. Yhteyksien tiedoista ilmoitetaan SSID, BSSID, taajuuskanava, signaalin voimakkuus, käytetty 802.11X-standardi ja käytetty salausprotokolla. Sivun viimeinen välilehti Configure sallii käyttäjän muokata muutamia tukiaseman asetuksia. Sivulta voi määritellä IP-asetuksia (Staattinen IP-osoite tai DHCP, määrätty VLAN), ottaa site survey -tilan käyttöön tai pois käytöstä, säätää molempien käytössä olevien radioiden (yksi 2,4 GHz radio ja yksi 5 GHZ radio) asetuksia (käytettävä taajuuskanava ja desibelivoimakkuus) ja ottaa käyttöön välityspalvelimen tilanteissa, joissa laite ei saa yhteyttä Ciscon pilvipalvelimeen. Välilehti vaatii turvallisuussyistä kirjautumisen. Ponnahdusikkuna ilmoittaa käyttäjätunnuksen olevan ”admin” ja että palveluun määritelty salasana löytyy Meraki Dashboard -sivulta. Kyseisen salasanan voi määritellä tai tarvittaessa tarkistaa Meraki Dashboardista Device configuration -osuudesta, Network-wide > Configure > General -välilehdeltä. Lisäominaisuutena sivuston vasemmassa reunassa on aina auki paneeli, joka kertoo kyseisen tukiaseman toiminnan tilan.

4 AeroHiven verkonhallinta-alusta

HiveManager On Premises Network Management on alkuperäinen verkonhallintaratkaisu, jossa alustaa käytetään fyysisen laitteen kautta. Tukiasemien hallinta on keskitettyä, mutta data ei kulje julkiseen pilveen ja tämä vaihtoehto vaatii yhden ylimääräisen laitteen hankinnan. Alusta on saatavilla myös virtuaalikoneena tai online-versiona. HiveManagerin virtuaalinen versio toimii yrityksen omissa tiloissa ja vain yrityksen omassa verkossa, mutta fyysisen laitteen sijaan hallinta-alusta toimii virtuaalisena tietokoneen kautta. HiveManager Online on täysin sama alusta kuin edellä, mutta palvelu toimii ilman fyysistä laitetta tai virtuaalikonetta, kokonaan verkossa AeroHiven pilven kautta. [57, s.6.] AeroHive on kehittänyt myöhemmin toisen hallinta-alustan, HiveManager NG Public Cloud:in. HiveManager NG toimii julkisessa pilvessä AeroHiven ylläpitämän pilvipalvelualustan kautta. HiveManager NG on AeroHiven ”uuden sukupolven” verkonhallintaratkaisu. AeroHive on rakentanut aikaisemman ratkaisunsa uudelleen tehden siitä soveltu-

van erityisesti verkoille, joissa on paljon mobiililaitteita. [58.] AeroHive on vielä jälkeenpäin julkaissut HiveManager NG:stä virtuaalisen version, joka toimii samalla tavalla, kuin alkuperäisen HiveManagerin virtuaalinen versio [59].

Julkisella ja yksityisellä pilviratkaisulla on omat etunsa ja haittansa, jonka takia yrityksen on hyvä tutustua molempiin vaihtoehtoihin, jotta yrityksen verkkoa tullaan hallitsemaan siten, miten se heille parhaiten sopii. Julkisen pilvipalvelun etuja ovat tehokkuus ja yksinkertaisuus, pienemmät kulut ja ajansäästö sekä se, että palvelua ei tarvitse huoltaa. Julkinen pilvipalvelu tarjotaan useimmiten palveluna internetyhteyden kautta ja siihen kuuluu kolmannen osapuolen tarjoama isännöinti ja ylläpito. Palvelu toimii selaimen kautta, ja laskutus on useimmiten kuukausittainen tai vuosittainen. Yrityksen ei siis tarvitse käyttää varoja fyysisten laitteiden ostamiseen, joka pienentää myös sähkölaskua, eikä myöskään ylimääräisten työntekijöiden palkkaamiseen järjestelmän valvontaa varten. Julkinen pilvipalvelu ei vaadi ylläpitoa eikä huoltoa, mikä säästää aikaa. Jos laitteita pitää konfiguroida uudelleen, jokin servereistä kaatuu tai vaatii uudelleenkäynnistystä, tämä voi viedä tunteja perinteisissä verkoissa. Virtuaalinen ja keskitetty hallinta mahdollistaa konfiguraatioiden vaihdon minuuteissa. Kaatuneen serverin voi vaihtaa nopeasti toiseen, ja palveluntarjoaja pitää laitteiden ohjelmistot ajan tasalla.

Julkisen pilven eduista huolimatta jotkin sen ominaisuudet voivat tehdä siitä sopimattoman joillekin yrityksille. Esimerkiksi, koska julkinen pilvipalvelu toimii internet yhteyden kautta, yhteyden nopeus on rajoitettu palveluntarjoajan tarjoaman nopeuden mukaisesti. Jos yritys tallentaa suuria määriä dataa tai siirtää paljon dataa, tarjottu nopeus ei välttämättä riitä. Tämän lisäksi asiakkaan pitää päästä käsiksi dataan nopeasti, mutta jos latausajat ovat hitaita, monikaan asiakas ei välttämättä suvaitse tätä. Toinen huomioitava asia on datan suojaus: vaikka useimman pilvipalvelun suojaus on ensiluokkaista, erittäin herkän datan, kuten finanssitiedot, hallinnan antamisen kolmannen osapuolen käsiin nähdään usein potentiaalisena vaarana. Yksityinen verkko antaa yritykselle paremmat mahdollisuudet hallitaan tietojaan, sillä yritys huolehtii verkon valvonnasta ja ylläpidosta itse. Pilven siirtoteho on huomattavasti parempi yksityisessä pilvessä, koska data ei kulje internetin kautta, ja laitteiden, verkon, ja datan tallennuksen suorituskyky voidaan määrittää yrityksen tarpeiden mukaisiksi. Koska esimerkiksi juuri AeroHivellä on julkinen ja yksityinen versio hallinta-alustoista, asiakkaalla on mahdollisuus valita itselleen myös hybridi vaihtoehto, jossa yritys käyttää julkista pilveä osalle tarpeistaan ja yksityistä pilveä toisille tarpeilleen. [60.]

4.1 AeroHiven pilviarkkitehtuuri ja Cooperative Control -protokolla

AeroHiven pilviarkkitehtuuri toimii kokonaan ilman kontrolleria. Piirisarjojen tehot kasvavat ja hinnat laskevat jatkuvasti, mikä mahdollistaa tehokkaampien tukiasemien kehittämisen. [61, s. 9.] AeroHive on luonut yhdessä tehokkaampien tukiasemien, ja Cooperative Control -protokollan kanssa, arkkitehtuurin, jossa ohjaustaso on täysin jaettu, mikä poistaa erillisen kontrollerin tarpeen. Cooperative Control -protokolla on esimerkiksi OSPF:n ja STP:n tapainen ohjausprotokolla, joka on kokoelma AeroHiven omia protokollia, ja nämä protokollat mahdollistavat ohjaustason toiminnot tukiasemissa [61, s. 9; 62, s. 6]. Arkkitehtuurissa ohjaus- ja datatasot kulkevat jokaisen tukiaseman välillä, hallintataso kulkee pilvestä tukiasemiin, ja datataso jatkaa edelleen tukiasemilta niihin liittyneisiin laitteisiin [61, kuva s. 9]. Hallintataso on säilytetty keskitettynä, koska se on tärkeä osa langattoman verkon tukemista ja asennusta [61, s. 9].

Cooperative control sisältää AMRP-, ACSP-, DNXP- ja INXP-protokollat. AMRP-protokolla (AeroHive Mobility Routing Protocol) mahdollistaa asiakkaan L2-vaeltamisen (siirtokerros), asiakastietojen älykkään jakamisen (istunnon tila, salausavaimet, ja identiteettitiedot), parhaan reitin valitsemisen mesh-linkkien välillä (best path forwarding), asiakkaiden eristämisen, paikannuksen, salasanojen luomisen RADIUS-serverin ja sen asiakkaiden välille (serverinä toimiva AeroHive -tukiasema ja sitä käyttävät muut tukiasemat), asiakkaiden kuormien tasaamisen (load balancing), tunnelien todennuksen ja liikenteen siirtämisen toimivaan tunneliin vikatilanteissa. ACSP-protokolla (Automatic Channel Selection Protocol) hallitsee tukiasemien dynaamista taajuuskanavien optimointia ja virta-asetuksia. DNXP-protokolla (Dynamic Network Extension Protocol) luo ja purkaa General Routing Encapsulation -tunneleita (GRE) AeroHive-laitteiden välillä L3-vaeltamista varten (verkkokerros). GRE-tunneli on mekanismi, jolla yhden protokollan paketteja voi siirtää toisen protokollan sisällä [63]. INXP-protokolla (Identity -based Network Extension Protocol) hallinnoi GRE-tunnelien luomista käyttäjien identiteetin, laitetyypin tai SSID:n perusteella. [64.]

4.2 Tukiasemat ja tekniset ratkaisut

AeroHiven kaksi uusinta tukiasemaa, AP250 ja AP245X, ovat ominaisuuksiltaan hyvin samanlaisia toistensa ja Ciscon MR42-tukiaseman kanssa. Molemmissa tukiasemissa

on kaksi radiota 2,4 GHz:n ja 5 GHz:n kanaville, 3x3:3 MU-MIMO ja SU-MIMO-ominaisuuksilla. Muita MR42:sien kanssa yhteneviä ominaisuuksia ovat esimerkiksi BLE, OFDM, ja 256-QAM-modulointi. [65;66.] AP245X-tukiasema on tarkoitettu vaativiin sisäolosuhteisiin, sen toimintalämpötila on korkeampi/matalampi, ja siinä on kolme antennia: yksi suuntaamaton antenni, yksi 60 asteen sektorin antenni ja yksi 120 asteen sektorin antenni [67]. AP250-tukiasema on tarkoitettu enemmän ”normaaliin” käyttöön, ja AeroHiven mukaan tukiasema sopeutuu alati vaihtuvaan verkkoympäristöön välittömästi. Tukiasema takaa parhaimman mahdollisen kattavuuden ja tehon. Tämän tukiaseman radioita voi käyttää tavallisesti, eli toinen radio toimii 2,4 GHz:n alueella ja toinen 5 GHz:n alueella, mutta myös niin, että molemmat radiot toimivat 5 GHz:n alueella [68].

Ominaisuuksia, joita ei mainita MR42-tukiaseman tiedoissa, ovat Trusted Platform Module (TPM), Integrated Application Visibility and Control (AVC) [67;68] sekä RF-IQ [68]. Lyhyesti kuvattuna AVC:llä tarkoitetaan sovellusten hallintaa HiveManager NG:n kautta. Hallinta-alustan kautta on mahdollista nähdä kaikki verkon tapahtumat sekä hallita, mitä sovelluksia sallitaan ja mitkä sovellukset ovat etusijalla [69]. RF-IQ on käytännössä vain kokonaisuus jo aikaisemmin mainittuja teknologioita, protokollia ja ratkaisuja, joiden avulla AeroHiven laitteet ja hallinta-alustat ylläpitävät verkon toiminnan tasoa koko ajan muuttuvassa radioympäristössä. Tähän kokonaisuuteen kuuluu esimerkiksi tukiasemien MIMO-ominaisuudet, ACSP-protokolla, band steering, load balancing, SLA-asetukset, ja Dynamic Airtime Scheduling. [70.] Trusted Platform Module on mikrokontrolleri-siru, joka säilöö verkkoavaimia, salasanoja, ja digitaalisia sertifikaatteja. TPM-sirun sisältämät tiedot salataan niin, että ne voi purkaa vain ylläpitäjän tunnuksilla. Vaikka laite joutuisi varastetuksi, tai muuten vaaran alaiseksi, kaikki sen sisältämä data on käyttökelvotonta ilman niiden salausten purkamiseen tarvittavia tunnuksia. [71.]

AeroHiven tukiasemat voivat tarvittaessa toimia RADIUS-serverinä, ja tarjota turvallisen WLAN-todennuksen 802.1X- ja EAP-protokollien avulla. RADIUS-ominaisuus poistaa tarpeen ostaa, konfiguroida, ja ylläpitää erillistä serveriä. Tukiasema voi käyttää todennukseen paikallista tietokantaa tai ulkoista hakemistopalvelua, kuten ActiveDirectory tai LDAP. Todennusavainten käsittely ja jako tapahtuvat paikallisesti tukiasemilla, mikä ei rasita verkon muita RADIUS-servereitä ja todennusprosessi tapahtuu kokonaan paikallisesti ilman, että liikenne kulkee WAN-verkon kautta [62, sivu 27].

Dynaaminen lähetysajan jakaminen (Dynamic Airtime Scheduling) on ratkaisu, joka säätelee sen ajan määrää, jonka jokainen käyttäjä saa datan lähettämiseen. Normaalisti

verkon toimintaa ja palvelun laatua yritetään parantaa säätämällä käyttäjille annettavan kaistan määrää. Tämä ei kuitenkaan oikeastaan paranna verkon suoritusta, koska se aika, joka käyttäjällä kuluu datan lähettämiseen, määrittää, kuinka kauan tämä käyttäjä vie kaistaa muilta käyttäjiltä. Eritoten hitaat käyttäjät kuluttavat niin paljon aikaa datan lähetykseen, että se vähentää muille käyttäjille jäävää lähetysaikaa. Tukiasema laskee lähetysajan käytön käyttäjien tietojen, käyttäjäjonojen, käyttäjäkohtaisen datanopeuden, ja kehyksen lähetysaikojen perusteella. Osalle käyttäjistä voi myös antaa etuaseman lähetysajan jaossa QoS-käytäntöjen kautta. Normaalisti dataa lähetetään lomittain, jokainen käyttäjä vuorotellen, mutta lähetysajan jakamista käytettäessä nopeamman käyttäjän annetaan suorittaa yksi lähetys loppuun asti, jonka jälkeen hitaammat käyttäjät jatkavat omia lähetyksiään, ja kaistalla on vähemmän käyttäjiä rasittamassa sitä [72, kuva]. Dynaamisen lähetysajan jakamiseen on liitetty myös Airtime boost -ominaisuus, jonka tarkoitus on pitää huolta siitä, että käyttäjän suoritusteho vastaa sovittua palveluntasoa. Jos käyttäjän profiiliin määritettyä palveluntasoa ei saavuteta, Airtime boost lisää käyttäjälle annettua lähetysaikaa lähetystehon parantamiseksi [62, s. 18-20].

4.3 HiveManager NG

HiveManager NG:ssä verkkoon kuuluvien laitteiden asetukset määritetään kokonaisuudessaan yhden verkkokäytännön alle (network policy). Verkkokäytäntö on kokoelma asetuksia, mikä voidaan asettaa yhtä aikaa usealle tukiasemalle tai kytkimelle, joilla on samanlaisia ominaisuuksia, kuten sijainti tai käyttötarkoitus. Kaikkein yksinkertaisimmillaan verkko tarvitsee toimiakseen vain yhden verkkokäytännön, johon on määritetty SSID ja laitesapluuna (device template). [73.]

SSID:eille löytyy samat todennus-protokollat kuin Merakille, sekä splash-sivu, ja Merakista poiketen myös Private Pre-Shared Key (PPSK). PPSK on ainutlaatuinen ennalta jaettu avain, jonka avulla jokaiselle käyttäjälle voidaan antaa oma avain. Jos avain täytyy jostain syystä vaihtaa, tai poistaa käyttäjältä, muutoksen voi tehdä vain tämän käyttäjän kohdalla ilman, että kaikkien käyttäjien avain täytyy muuttaa. [74.] SSID:lle täytyy määrittää myös yksi käyttäjäprofiili, jonka SSID asettaa käyttäjille oletuksena, kun he liittyvät verkkoon. Käyttäjäprofiili sisältää VLAN-, GRE -tunnelointi-, QoS- ja SLA-asetuksia, sekä asetukset siitä milloin, kuinka kauan ja millä data-rajoituksella SSID on käytössä. [75.] Jos käyttäjäprofiileja halutaan luoda useampia, valitun todennustavan täytyy olla WPA/WPA2 802.1X (Enterprise), WEP-802.1X, MAC-todennus, tai splash-sivu, ja tämä

profiili voidaan asettaa käyttäjille RADIUS-serveriin määritetyn ryhmän, MAC-osoitteen, käyttäjän laitteen käyttöjärjestelmän, tai paikallisen käyttäjäryhmän perusteella [76]. HiveManagerissa on kaksi erilaista käyttäjäryhmää RADIUS-serverin kautta asetetuille profiileille ja paikallisille käyttäjäryhmille. RADIUS-serverin kautta profiileihin liitettäviin ryhmiin määritetään salasanat sisältävän tietokannan sijainti (pilvi tai paikallinen tukiasema), salasanojen ominaisuudet, ja jakotapa. [77.] Paikallisiin käyttäjäryhmiin määritetään, miten salasanat luodaan (manuaalinen tai automaattinen) ja salasanojen ominaisuudet [78]. Tämä lähestymistapa vaikuttaa turhan monimutkaiselta Merakiin verrattuna ja AeroHiven dokumentaatio on osittain puutteellinen, mikä vaikeuttaa profiilien ja ryhmien konkreettisen toiminnan hahmottamista, ja näiden ominaisuuksien määrittämistä.

Laitesapluuna on diagrammi tietyn tukiaseman tai kytkimen fyysisistä porteista, jonka avulla voidaan määrittää portin tyyppi ja toiminta [79]. Fyysisen portin voi asettaa kolmeen tilaan: bridge-access, bridge-802.1Q ja uplink port. Bridge-access-tilaa käytetään silloin, kun porttiin on liitetty yksittäinen käyttäjä (host), ja tähän määritetään tapa, jolla käyttäjä todennetaan. Bridge-8021Q -portti toimii siltana internet-yhteyden jakamista varten, ja portti tukee useita VLAN:eja. Uplink port on portti, joka on liitetty suoraan WAN-verkkoon. [80.] Toisin kuin Merakissa, laitesapluuna sisältää myös radioprofiilin, jolla määritetään tukiaseman radioiden toiminta, kuten radioiden optimointi, load balancing- ja band steering-ominaisuudet, taajuuskanavien automaattinen vaihto, radioiden toiminta vikatilanteissa [79], liikenteen priorisointi WMM:n avulla, ja ympäristön analysointi, eli WIPS-alustan ja L3-vaelluksen toimintaan liittyvät skannaukset [81].

SSID:lle voi vielä määrittää monia valinnaisia asetuksia, kuten suodattaa hallinta ja diagnostiikka liikennettä (esimerkiksi SSH ja SNMP), asettaa prioriteetin tietylle käyttäjäprofiilille silloin, kun vaihtoehtoja on useampia, optimoida verkon toimintaa ääniliikenteen osalta, ottaa WMM-asetukset käyttöön video- ja/tai ääniliikenteen kohdalla, sallia multicast-liikenteen muuttamisen unicast-liikenteeksi video-dataa lähetettäessä käytettävissä olevan lähetysajan säästämiseksi, muuttaa käyttäjiin liittyviä asetuksia, kuten korkein sallittu käyttäjien määrä ja datan lähetykseen liittyvät asetukset ja muuttaa tukiasemien välillä tapahtuvaan käyttäjien vaeltamiseen liittyvien välimuistien sisältämien tietojen säilytysaikaa. Huomattavana erona Merakiin SSID:n valinnaisista asetuksista voi vaihtaa myös radioiden tukemia nopeuksia ja modulaatiota ja määrittää yksityiskohtauksen suojauksen DoS-hyökkäyksiä vastaan. [82.]

5 Aruban verkonhallinta-alustat, tukiasemat ja ratkaisut

AeroHiven tapaan Aruballa on useita vaihtoehtoja tukiasemien hallintaan: Aruba Instant, Aruba AirWave ja Aruba Central. Aruba Instant on suoraan Aruban tukiasemien nimi, joihin yleensä viitataan lyhenteellä IAP (Instant Access Point). Tukiasemissa on itsessään selainpohjainen GUI, jonka kautta tukiasemille ja verkolle voi asettaa lähes kaikki samat ominaisuudet kuin erillisen hallinta-alustankin kautta. [83.] Tätä GUI:ta ei kuitenkaan ole tehty verkon valvontaa varten, joten kaikkia hallinta-alustoille ominaisia tilastoja sekä yms. ei ole. Poikkeuksena graafi taajuuskanavien laadusta, käytettävyydestä, ja käytöstä. [84.] Aruban tukiasemat eivät AeroHiven ja Ciscon tapaan tarvitse erillistä fyysistä kontrolleria, mutta Aruban tapauksessa yksi tukiasemista voidaan asettaa, tai saa automaattisesti, virtuaalisen kontrollerin rooliin. Virtuaalinen kontrolleri koordinoi, säilyttää ja jakaa kaikki ne asetukset, joita verkon keskitetty hallinnoiminen vaatii. [85.] Virtuaalinen kontrolleri on selkeästi hyödyllinen, jos tukiasemia hallitaan Instant-GUI:n kautta, koska se mahdollistaa konfigurointien keskitetyn jakamisen. Virtuaalinen kontrolleri on kuitenkin Aruban dokumentaation mukaan käytössä vielä yrityksen pilvihallinta-alustassa, mutta van muutama asetus liittyy sen käyttöön, joten esimerkiksi sen tarpeellisuus on kyseenalainen.

Aruba AirWave on Aruban ensimmäinen hallinta-alusta, joka oli ja on edelleen Aruban ”on-premises”-vaihtoehto [86]. Aruban lyhyt esittely AirWavesta viittaa siihen, että tämä alusta antaa käyttäjälle paremman näkyvyyden verkon tapahtumiin ja samalla paremmat mahdollisuudet verkon yksityiskohtaiseen hallintaan kaiken saatavilla olevan datan avulla. Alusta kerää dataa esimerkiksi käyttäjien yhteyden laadusta, RADIUS-serverin todennus ajasta, DHCP-serverin toiminnasta ja nimipalvelimen-toiminnasta. Normaalin sovellus hallinnan ja valvonnan lisäksi AirWave seuraa erityisesti kommunikointisovelluksia, kuten Skype for Business ja kaikkia verkon WiFi-puheluita. Yksi AirWaven ainulaatuisista ominaisuuksista on VisualRF, joka kartoittaa tarkasti koko radioympäristöstä jokaisen verkkoon liittyneen laitteen, niiden sijainnin ja verkon suorituksen. [87.] AirWaven dokumentaatio antaa kuitenkin sellaisen kuvan, että alustan teossa itse WLAN-verkon ominaisuuksiin ei ole kiinnitetty paljon huomiota, mahdollisesti siksi, että alusta on vanhempi ja sen ominaisuuksia ei ole päivitetty nykyaikaisten WLAN-verkkojen vaatimusten mukaisiksi. Alustan tarjoamat ominaisuudet ovat myös osaltaan sidonnaisia muiden yritysten tarjoamiin kontrollereihin, dokumentaatiossa mainittuna Cisco, Proxim, ja Symbol. [88.]

Aruban uusin hallinta-alusta on pilvipohjainen Aruba Central, joka on selkeästi suunniteltu nykyaikaisia BYOD-verkkoja ajatellen. Central on kuitenkin ominaisuuksiltaan ja ratkaisuiltaan hyvin yleislaatuinen. Siinä missä Centralista löytyy melkein kaikki samat perusominaisuudet, mitä tulee esimerkiksi todennukseen, suojaukseen ja radioiden-asetuksiin kuin Ciscon Merakista ja AeroHiven HiveManager NG:stä, tästä alustasta ei kuitenkaan nouse samalla tavalla esille mitään ratkaisuja tai tekniikoita, jotka Aruba olisi itse kehittänyt, toisin kuin Ciscon ja AeroHiven kohdalla. Myös osa tavasta, miten Aruba on toteuttanut Central-alustan, saattaa rajoittaa verkon suunnittelua.

Aruban nimeämiä omia ratkaisuja ovat AppRF ja Adaptive Radio Management (ARM). AppRF on sovellusympäristöä hallinnoiva kokonaisuus tekniikoita ja ominaisuuksia, jonka avulla voi luoda sovelluksia, palveluita, ja internetsivuja koskevia palomuurisääntöjä. AppRF toimii tukiasemien kautta, jotka käyttävät Deep Packet Inspection -teknologiaa (DPI) pakettien tunnistuksessa [89, s. 111]. DPI on teknologia, jonka avulla on mahdollista tutkia datapaketteja syvemmin kuin pelkästään paketin osoitekentän tietoja [91]. Sovelluksille voi myös luoda kaistaa rajoittavia käytäntöjä ja QoS-käytäntöjä. Kuvaillut ominaisuudet ovat hyvin samanlaisia kuin Merakin L7-palomuurisäännöt ja traffic shaping -ominaisuus. AeroHiven kohdalla sovellusten hallinasta ei ole tehty erityistä kokonaisuutta, mutta HiveManager NG tarjoaa kokonaisvaltaisen näkymän verkossa käytettyihin sovelluksiin, joita on mahdollista esimerkiksi ryhmitellä ja käyttää luotuja ryhmiä IP-pohjaisissa palomuurisäännöissä [91;92].

Adaptive Radio Management on Aruban tukiasemien käyttämä ratkaisu WLAN-verkon suorituskyvyn optimointia varten. Kuten Meraki ja HiveManager NG, ARM sisältää dynaamisen taajuuskanavien ja tehoasetusten säätämisen. Kun ARM on käytössä, tukiasema skannaa kaikkia 802.11-kanavia tasaisin väliajoin tutkiakseen verkon kattavuutta, häiriöitä, ja myös mahdollisten tunkeilijoiden varalta. Tämän takia ARM on suunniteltu niin, että skannausta ei suoriteta, jos tukiasemalla on edes yksi aktiivinen puhelu, ja se sisältää ominaisuuden, joka tarvittaessa muuttaa skannaus-käyttäytymistä dynaamisesti. ARM:n yhteyteen on vielä luotu ClientMatch-ominaisuus, joka sisältää load balancing- ja band steering -asetukset, ja tukiaseman välillä liikkumista tukevia asetuksia. Näiden yhteyteen kuuluu vielä kolmantena Airtime Fairness Mode, joka takaa kaikille käyttäjille yhtäläisen pääsyn kaistalle laitteen ominaisuuksista huolimatta. Ominaisuuden tarkoitus on estää yhtä, tai muutamaa käyttäjää, viemästä koko verkon suorituskykyä. Airtime Fairness Mode on verrattavissa AeroHiven Dynamic Airtime Scheduling -ominaisuuteen, mutta AeroHiven ratkaisu on toteutettu eri tavalla. [89, s. 59-60.]

Ainakin kolmella Aruban tukiasemasarjalla, 330, 320, ja 310, on nopean vertailun perusteella lähes samat ominaisuudet, ja näistä lähempään tarkasteluun valittiin 330-sarja. 330-sarjan tukiasemat ovat jälleen hyvin samanlaisia kuin muutkin tässä työssä käsitellyt tukiasemat. Tukiasemissa on kaksi radiota, 4x4:4 MU-MIMO ja SU-MIMO, beam forming, DFS, OFDM, 256-QAM-modulointi, BLE ja TPM. Ciscosta ja AeroHivestä poiketen Aruban tukiasemissa on Intelligent Power Monitoring -ominaisuus, joka valvoo tukiaseman virrankäyttöä, ja tarvittaessa ottaa joitain tukiaseman ominaisuuksia (esimerkiksi USB-portti) pois käytöstä käytettävissä olevan virran määrän perusteella. [93.] ClientMatch-teknologiaa on paranneltu 802.11ac Wave 2 -standardia ja MU-MIMO:a ajatellen niin, että ne laitteet, jotka tukevat tätä standardia, ohjataan automaattisesti samaa standardia tukeville tukiasemille, jotta kaikki MU-MIMO:a tukevat laitteet voivat hyödyntää sitä [93;94].

5.1 Aruba Central

Tukiasemalle itselleen määritetään radioprofiili, joka sisältää tukiaseman perustiedot, kuten nimen, staattisen tai DHCP:ltä saatavan IP-osoitteen ja radioiden tilan. Radioiden tila voi olla access, monitor tai spectrum monitor. Access-tilassa käyttäjät voivat muodostaa yhteyden tukiasemaan ja tukiasema suorittaa WIDS-skannauksia, monitor-tilassa käyttäjät eivät voi yhdistää tukiasemaan ja tukiasema tarkkailee ympäristöä luvattomien käyttäjien varalta ja spectrum monitor -tilassa tukiasema valvoo radioympäristön häiriöitä. ARM-ominaisuus on käytössä automaattisesti, joka asettaa radio-profiilille sopivat taajuuskanavat ja tehoasetukset. [89, s. 40.]

Centralissa verkolle luodaan SSID-profiili, jonka perusasetuksista valitaan verkolle tyyppi, joka tässä tapauksessa on langaton, ja verkon käyttötarkoitus, joka voi olla työntekijöille, ääniliikenteelle tai vierailijoille suunnattu verkko. Työntekijöille suunnattu verkko on tavanomaisin verkkotyyppi, mikä käyttää todennustapanaan salasanaa tai 802.1X:n pohjautuvia todennustapoja. Ääniverkko on tarkoitettu laitteille, jotka tarjoavat vain äänipalveluja, kuten matkapuhelimille tai sovelluksille, jotka vaativat ääniliikenteen priorisointia. Vieraille, eli ne henkilöt, jotka käyttävät yrityksen verkkoa, mutta eivät ole yrityksen työntekijöitä, suunnattu verkko käyttää todennustapana salasanaa tai splash-sivua. Tavallisesti tällaisen verkko ei käytä mitään salausta, mutta Centralissa vierasverkolle on mahdollista määrittää salaus. [89, s. 44.] Jos tukiaseman täytyy tukea langallisia käyttäjiä, myös lankaverkkoon liitetylle portille määritetään profiili [89, s. 56].

SSID:lle voi määrittää esimerkiksi broadcast- ja multicast-liikenteen hallintaan vaikuttavia asetuksia, taajuusalueiden minimi- ja maksimi-lähetysnopeudet, taajuusalueet, kaistan rajoituksen, käyttäjien maksimimäärän ja yhteyden aikakatkaisun, WMM-asetukset ja SSID:n mainostuksen. Näiden lisäksi SSID:lle määritetään VLAN-asetukset, suojaus ja palomuuri/pääsylistat (Access Control List, ACL). [89, s. 45-50.] Verkon suojauksessa verkolle valitaan suojauksen taso, joka voi olla enterprise, personal, tai open. Central tukee kaikkia tavanomaisia salaus- ja todennustapoja kuten WPA2- ja WPA-Enterprise, MAC-todennus, 802.1X, ja splash-sivu. Centralista löytyy vielä WISPr-todennus (Wireless Internet Service Provider roaming). WISPr tukee langattomien laitteiden liikkumista eri palveluntarjoajien verkkojen välillä, ja sallii yhteyden muodostamisen sellaistenkin palveluntarjoajien verkkoihin, joiden kanssa laitteen haltijalla ei ole tiliä [89, s. 69]. Valittavissa oleva todennus on kuitenkin rajoitettu sen mukaan, mikä suojauksen taso on valittu. [89, s. 47-49.]

Centralin palomuuri käyttää pääsylistoja liikenteen hallintaan. Centralissa pääsylistoilla on mahdollista määrittää pääsy verkkoon ja sen osiin, sallia tai kieltää pakettien kulku tukiaseman läpi, luoda tiettyjä palveluja, sovelluksia ja internetsivuja koskevia sääntöjä. Pakettien kohdalla käytetään ensimmäistä niihin soveltuvaa sääntöä, niin kuin palomuurisäännöt tavallisestikin toimivat. [89, s. 76.] ACL:t voidaan asettaa voimaan verkon laajuisesti, eli kaikille kyseisen verkon käyttäjille tai tietyille käyttäjille käyttäjäroolien perusteella [89, s. 50]. Käyttäjärooleihin voi vielä määrittää, kuinka usein käyttäjä todennetaan uudelleen, ja niihin on mahdollista liittää ”sopimus” kaistan nopeudesta. Roolit annetaan käyttäjille sääntöihin määritettyjen ominaisuuksien mukaisesti, esimerkiksi MAC-osoitteen tai laitteen valmistajan mukaan (DHCP fingerprinting). [89, s. 78-80.] Centralissa myös NAT kuuluu pääsylistalla määritettäviin toimintoihin, ja Central tukee myös NAT:n yhteydessä käytettävään Application Layer Gateway -toimintoon (ALG) [89, s. 76]. NAT:n tarkoitus on suorittaa osoitteiden muutos kokonaan niin, että se ei vaikuta mitenkään verkon toimintaan, mutta tämä ei aina ole mahdollista, jolloin NAT tarvitsee avukseen jonkin ALG-protokollan, kuten Voceran tai Cisco Skinnyn [95, s. 1;89, s. 76]. Jos SSID:n halutaan olevan käytössä vain tiettyinä ajankohtina, tämäkin määritellään erilliseen Time Based Services -profiiliin, joka liitetään SSID:een [89, s. 58-59].

Centralin WIDS-ominaisuus etsii verkosta luvattomia ja häiriötä aiheuttavia tukiasemia sekä muita laitteita, jotka saattavat häiritä verkon toimintaa. Centralin WIDS:n mukaan luvaton tukiasema on tukiasema, joka on liitetty yrityksen lankaverkkoon, ja häiriötä ai-

heuttava tukiasema on tukiasema, joka havaitaan langattomassa verkossa, eikä ole liitetty lankaverkkoon. Järjestelmälle luodaan käytäntöjä, joiden perusteella määritetään, mitä uhkia verkosta etsitään ja miten tukiasemia sekä käyttäjiä suojataan uhilta. Tässäkin tapauksessa käytäntö määritetään niin, että sille valitaan suojauksen taso, joka puolestaan automaattisesti määrää, mitä uhkia etsitään ja miten suojaudutaan, eli ylläpitäjä ei voi luoda kaikista tuetuista vaihtoehdoista omaa kokonaisuutta. Lopuksi järjestelmälle määritetään tapa, jolla havaittuja uhkia hallitaan. [89, s. 64-66.] Asetuksista ei löydy mahdollisuutta määrittää, miten ja milloin WIDS-skannauksia suoritetaan eritoten silloin, kun tukiasema on access-tilassa.

6 Yhteenveto

Insinöörityössä tutustuttiin Cisco Systemsin, AeroHive Networksin ja Aruba Networksin tarjoamiin pilvipohjaisiin verkonhallinta-alustoihin ja pilven kautta hallittaviin tukiasemiin. Alustojen ja tukiasemin ominaisuudet ja toteutus käytiin läpi mahdollisimman tarkasti niin, että jokaisen yrityksen vaihtoehtoja voisi verrata keskenään parhaimman vaihtoehdon löytämiseksi. Työn teon yhteydessä Metropolia Ammattikorkeakoululle tilattiin opetuskäyttöön neljä kappaletta Ciscon Meraki-sarjan MR42-tukiasemia, joten Ciscon alustaa oli mahdollista tutkia lähemmin. AeroHiven ja Aruban alustoihin tutustuttiin molempien yritysten dokumentaation ja konfigurointi ohjeiden kautta. Tukiasemista tutkittiin niitä tukiasemia, jotka olivat uusimpia jokaisen yrityksen valikoimassa. Työtä tehdessä Ciscon MR42-tukiasema oli yrityksen uusimpia, mutta Cisco on myöhemmin julkaissut uusia malleja.

Koska Ciscon alustaa oli mahdollisuus käyttää insinöörityötä tehdessä, työn pääosuus keskittyy Meraki-alustan toteutuksen (miten alustalla konfiguroidaan verkko) ja ominaisuuksien sekä MR42-tukiasemassa käytettyjen teknisten ratkaisujen yksityiskohtaiseen kuvailuun. Insinöörityön kahdessa viimeisessä kappaleessa käydään läpi AeroHiven ja Aruban alustan sekä tukiasemien ominaisuudet, ja katsotaan, mitkä ominaisuudet ovat samoja/samanlaisia jokaisessa alustassa ja tukiasemassa ja mitä ainutlaatuisia ominaisuuksia niistä löytyy. Jokaisen yrityksen kohdalla kävi ilmi, että alustoissa ja tukiasemissa on paljon samoja ominaisuuksia, mutta osa näistä on selkeästi pakollisia toimivan ja kilpailukykyisen järjestelmän toteuttamiseksi. Näihin kuuluu esimerkiksi tukiasemien tukemat standardit, MU-MIMO, WIDS/WIPS-ominaisuudet, liikkeessä olevien käyttäjien

yhteyttä ylläpitävät ominaisuudet, palomuurit sekä tukiasemien kyky valvoa radioympäristöä ja muuttaa radioiden asetuksia dynaamisesti.

Asiat, jotka erottelevat jokaisen yrityksen järjestelmät toisistaan on yritysten omat ratkaisut alustojen toteutuksessa ja ne tekniset ratkaisut, jotka he ovat itse kehittäneet, tai vaihtoehtoisesti nähnyt tärkeäksi sisällyttää omaan kokonaisuuteensa. Näiden perusteella Aruban toteutus ei näytä yltävän samalle tasolle kuin AeroHiven ja Ciscon. Aruban omat ratkaisut, AppRF, Adaptive Radio Management ja Airtime Fairness Mode, ovat hyvin geneerisiä, ja niiden sisältämät ominaisuudet ovat AeroHiven ja Ciscon järjestelmissä perusominaisuuksiin lukeutuvia. AeroHive ja Cisco ovat myös kehittäneet näitä ominaisuuksia pidemmälle kuin Aruba. Ciscolla ei ole mitään Airtime Fairness Moden kaltaista tekniikkaa, mutta se on verrattavissa AeroHiven Dynamic Airtime Scheduling -ominaisuuteen, joka on kuitenkin toteutettu huomattavasti paremmin ja jolla on suurempi vaikutus verkon toimivuuteen. Valitettavasti Aruban dokumentaatio on epäselvää ja osittain puutteellista: dokumentaation perusteella verkon konfigurointi voi osoittautua monimutkaiseksi eikä lukijalle anneta täydellistä tietoa kaikista mahdollisista määritettävistä asetuksista.

Ciscon järjestelmä ja dokumentaatio ovat selvästi helpompia ymmärtää, mutta tämä voi johtua siitä, että epäselviä asioita voitiin vielä tarkistaa itse alustasta. Ciscon järjestelmä sisältää paljon samoja ominaisuuksia kuin Aruban ja AeroHiven, mutta yritys on kehittänyt osaa näistä pidemmälle niin, että niistä saadaan enemmän hyötyä. Cisco on myös panostanut omien ratkaisujensa kehittämiseen, mutta tähän mennessä toteutetut ominaisuudet eivät välttämättä erottele yritystä muista. Alustaan ja tukiasemiin valitut ominaisuudet keskittyvät Ciscon Bring Your Own Device -ratkaisun ympärille niin, että verkkoon liittyviä laitteita olisi mahdollisimman helppo hallita ja valvoa. Jokainen kolmesta järjestelmästä käyttää laitteiden ja sovellusten tunnistusta, mutta näiden lisäksi Cisco on kehittänyt vielä CMX Location Analytics -ratkaisun, ja tukiasemista löytyy vielä integroitu spektrianalysaattori sekä kolmas radio verkon valvontaa varten.

CMX ei ole mitenkään välttämätön ratkaisu yrityksille, sillä Meraki-alusta antaa jo itsessään hyvän näkymän verkon käytön osalta, mutta kolmas radio sekä spektrianalysaattori ovat erittäin tärkeitä radioiden dynaamisten ominaisuuksien ja WIDS/WIPS-alustan kannalta. Ciscon Systems Manager -työkalu on maininnan arvoinen, sillä se helpottaa yrityksen omien kannettavien laitteiden hallintaa huomattavasti, mutta valitettavasti työkalu

ei ole ilmainen vaan vaatii lisenssin. Ciscon WIDS/WIPS -alusta, Air Marshal, on mahdollisesti yrityksen suurin oma ratkaisu. Aerohivellä ja Aruballa on myös WIDS/WIPS-toiminnot, mutta näistä kaikista jokainen toimii osittain eri tavalla. AeroHiven ja Aruban toiminnoilla voi valita, mitä uhkia valvotaan ja niillä voi myös havaita laitteita, joiden asetukset eivät ole kohdillaan. Air Marshalissa tämä ei ole mahdollista, mikä saattaa vaikuttaa rajoitteelta, mutta Cisco on kuitenkin pitänyt huolen, että alustalla valvotaan automaattisesti kaikkia varteenotettavia uhkia ja hyökkäystapoja. Lisäksi Air Marshal pystyy valvomaan myös erinäisiä laitteita, joiden ei tulisi ikinä liittyä muuhun kuin yrityksen verkkoon, kuten esimerkiksi viivakoodinlukijoita. AeroHiven kohdalla huomioitavaa on, että jostain syystä DoS-hyökkäysten esto ei kuulu WIDS/WIPS-ominaisuuksiin, vaan SSID:n asetuksien alle. Ciscon tukiasemat olivat tutkituista vaihtoehdoista ainoat, jotka tukevat mesh-verkkoja. Niistä yritykset, jotka haluavat WLAN-verkon myös tiloihin, joihin sitä ei normaalisti olisi mahdollisuutta toteuttaa, saavat erityisen hyödyn. Tapa, jolla Meraki-alustassa konfiguroidaan verkko, on selkein kaikista kolmesta. Ainakin tutkittujen ominaisuuksien perusteella järjestelmä on onnistuttu toteuttamaan niin, että verkon hallinta ja valvonta ovat helppoa laadusta tinkimättä.

AeroHiven HiveManager NG -alustan toteutus vaikuttaa ensisilmäyksellä yksinkertaiselta: verkko tarvitsee toimiakseen vain verkkokäytännön. SSID:n määrittely kuuluu luonnollisesti verkkokäytännön alle, mutta tämän lisäksi käytännölle on pakollista määrittää vielä laitesapluuna, SSID:n alle käyttäjäprofiili, laitesapluunan alle radioprofiili, ja jos käyttäjäprofiileja on useampia, niiden kanssa voi vielä käyttää käyttäjäryhmiä. Ylläpidon näkökulmasta alustan käyttäminen vaatii uusien termien omaksumista. Verkon konfiguroimiseen kuuluu useita vaiheita, ja tarjolla oleva dokumentaatio ei aina anna selkeää kuvaa siitä, miten jotkin ominaisuudet toimivat tai mitä kaikkea pitää konfiguroida, jotta jokin ominaisuus on käytössä. Alustan monimutkaisuus ja puutteet dokumentaatiossa ovat AeroHiven kompastuskiviä, mutta muuten AeroHiven järjestelmä on ehkä jopa paras kaikista kolmesta. Usea AeroHiven valitsemista ominaisuuksista ja ratkaisuista osoittaa, että yritys pitää verkon suojausta tärkeänä. HiveManager-alusta toimii myös yksityisessä, joka suojaa asiakasyrityksen dataa, tukiasemat on suojattu TPM-sirulla, järjestelmässä on WIDS-ominaisuus, jolla on mahdollista havaita luvattomia asiakkaita ja tukiasemia, ja laitteita, joiden asetukset eivät vastaa vaatimuksia, SSID:n asetuksiin on mahdollista määrittää lukuisia DoS-hyökkäyksiä estäviä asetuksia, ja muista yrityksistä poiketen AeroHive käyttää PSK-avaimen sijaan PPSK-avainta. AeroHive on myös kilpailijoidensa edellä, mitä tulee teknologiaan: yritys on kehittänyt useita omia protokollia, joiden avulla tukiasemat toimivat ilman kontrolleria, eli jos pilveen ei saada yhteyttä, se ei

vaikuta verkkoon mitenkään. Toinen huomattava ero Ciscoon ja Arubaan on tapa, jolla AeroHiven tukiasemat lähettävät dataa: Dynamic Airtime Scheduling vähentää hitaampien käyttäjälaitteiden vaikutusta verkon nopeuteen huomattavasti ja vapauttaa kaistaa nopeammin. Kuten aikaisemmin mainittiin Aruban Airtime Fairness Mode takaa vain yhtäläisen kaistan jokaiselle käyttäjälle, eikä Ciscolla ole tällaista ratkaisua ollenkaan. Tukiasemien erityisominaisuutena ne voivat toimia myös RADIUS-serverinä. AeroHiven tekninen osaaminen vaikuttaa kiistattomalta, mutta ilman konkreettista kokemusta on vaikea sanoa kuinka paljon esimerkiksi juuri Dynamic Airtime Scheduling vaikuttaa verkon suorituskykyyn.

Kaikkea näistä kolmesta kokonaisuudesta opittua on hyvä miettiä kahdesta näkökulmasta: uutta verkkoratkaisua etsivän asiakkaan näkökulmasta ja ylläpidon näkökulmasta. Työssä ja yhteenvedossa esiin tulleet ongelmat eivät välttämättä vaikuta asiakkaan päätökseen, jos asiakkaan ei ole tarkoitus ylläpitää verkkoa itse, sillä heidän ei tarvitse huolehtia verkon ylläpidosta. Asiakkaan on tietenkin hyvä tutustua jokaiseen vaihtoehtoon, ja tutustua myös tarjolla oleviin kokeiluversioihin, mutta jokaisen tutkitun kokonaisuuden perusominaisuudet ovat niin samanlaiset, että niistä jokaisella voi muodostaa yhtä toimivan, tavallisiin tarpeisiin sopivan, verkon. Tämä on hyvä, sillä ne asiakkaat, joilla on ennestään laitteita joltakin näistä yrityksistä, on luonnollisempaa valita sama yritys uudestaan. Tästä näkökulmasta Aruban ja Ciscon kokonaisuuksilla ei ole huomattavasti eroa. Molemmat yritykset käyttävät pilvikontrolleria, joten tältä osalta verkon luotettavuus on samalla tasolla, mutta loppujen lopuksi Ciscon kehittyneemmät ominaisuudet ovat paremmat kuin mitä Aruba tarjoaa. AeroHive on heti ensimmäinen vaihtoehto asiakkaille, jotka haluavat käyttää pilvipalveluita yksityisen pilven kautta ja asiakkaille, jotka haluavat panostaa verkkonsa turvallisuuteen. Lisäksi Dynamic Airtime Scheduling tekee AeroHiven verkosta teoriassa parhaiten toimivan ja yrityksen kontrolleriton arkkitehtuuri lisää verkon luotettavuutta huomattavasti.

Asiakkaan oman ylläpidon kannalta esiin tulleet ongelmat voivat vaikuttaa asiakkaan päätökseen paljon enemmän. On todennäköistä, että ylläpidolle annetaan tehtäväksi etsiä asiakkaan tarpeille parhaiten sopiva vaihtoehto, mikä on huomattava etu. Ylläpidolla on taito ymmärtää jokaisen vaihtoehdon edut, henkilökohtainen kokemus siitä, mitä asiakkaan verkko tarvitsee, ja myös oma mielipide siitä, millaisella alustalla he haluavat hallita verkkoa. Ominaisuuksien kannalta ylläpidon kannattaa edelleen valita asiakkaan tarpeille parhaiten sopiva vaihtoehto. Tästä näkökulmasta alustojen toteutus voi kuitenkin olla vaikuttava tekijä. Insinöörityössä tehdyn tutkimuksen aikana selvinneet ongelmat

Aruban ja AeroHiven dokumentaatiossa saattavat ja itsessään vaikuttaa ylläpidon päätökseen: jos verkon konfigurointi ja hallinta koetaan monimutkaiseksi, ylläpidon työ vaikeutuu. Mutta kuten aikaisemmin mainittiin, AeroHiven tarjoamat ominaisuudet voivat olla asiakkaalle paljon tärkeämpiä kuin alustan käytettävyys. Tutkituista alustoista Ciscon Meraki vaikuttaa parhaiten toteutetulta. Verkon konfigurointi on jäsennelty selkeästi ja itse alusta sisältää tarpeeksi infoa, joten verkon voi konfiguroida ilman, että dokumentaatioon täytyy tukeutua koko ajan. Tukiasemien automaattisesti tai dynaamisesti toimivat ominaisuudet vähentävät verkon aktiivisen hallinnan tarvetta, ja tapa, jolla alusta esittää verkosta kerättyä dataa verkosta, käyttäjistä, ja radioympäristöstä, mahdollistaa verkon erittäin tarkan valvonnan.

Kaiken yhteenvedossa mainitun jälkeen on hyvä mainita vielä kerran, että Aruban ja AeroHiven järjestelmistä todetut asiat ovat muodostettu vain yritysten dokumentaation perusteella, koska itse alustoja ei testattu insinöörityön teossa. Myöskään kaikkien mainittujen ominaisuuksien ja tekniikoiden konkreettista toimivuutta ei mitenkään voitu testata, joten varsinkin yritysten omien ratkaisuiden hyödyt tiedetään vain sellaisinaan, kuin yritysten dokumentaatio tuo ne esille. Yritysten ratkaisuja on vaikea tuoda esille positiivisessa tai negatiivisessa valossa, sillä jokaisella asiakkaalla on omat tarpeensa. Esimerkiksi asiakas voi haluta itselleen vain pienen, yksinkertaisen verkon, milloin esimerkiksi AeroHiven tarjoamilla ominaisuudet ei ole paljon arvoa ja Aruban kokonaisuus saattaa olla juuri sopiva, insinöörityössä huomatuista ongelmista huolimatta. Insinöörityön lopullisena yhteenvetona voidaan sanoa, että minkä tahansa yrityksen asiakas valitseekin, pilvipohjaisen verkkoratkaisun valitseminen kannattaa. Siinä missä kontrollerin käyttäminen verkossa, fyysisen tai virtuaalisen, on edelleen täysin käypä ratkaisu monelle yritykselle, pilvipohjainen verkko kuitenkin poistaa suurimman osan kontrollerin käyttöön liittyvistä ongelmista, sekä ongelmista, joita langattoman verkon ylläpitämisessä on nykyaikana. Vaikka asiakkaan verkkotarpeet eivät vaatisi tukea lukuisille langattomille laitteille, pilvipohjainen verkko on silti kannattava valinta. Pilvipohjainen ratkaisu lisää verkon turvallisuutta ja luotettavuutta, sekä vähentää asiakkaan kuluja. Asiakkaille, joiden tarpeet ovat suuremmat, pilvipohjainen verkko on ehdottomasti oikea suunta. Isojen WLAN-verkkojen luotettavuus, hallittavuus, ja valvottavuus ovat kriittisiä ominaisuuksia. Pilvipohjaiset ratkaisut ovat suunniteltuja juuri näihin tarkoituksiin. Lisäksi kuluissa säästäminen tulee vielä paremmin esille, kun ratkaisu on laaja, ja verkko on helpompi toteuttaa useampaan kohteeseen, tai kohteisiin, joihin verkon toteuttaminen on vaikeaa aikaisemmilla ratkaisuilla.

Lähteet

1 Tetz, Edward. Cisco Enterprise Infrastructure Access Points. Verkkoartikkeli. For Dummies. <http://www.dummies.com/programming/networking/cisco/cisco-enterprise-infrastructure-access-points/>. Luettu 31.10.2016.

2 Controllers, Cloud, & Cooperative Control. 2015. Verkkodokumentti. AeroHive Networks, Inc. <http://media.aerohive.com/documents/1037869545_Aerohive-Whitepaper-Controllers-Cloud-Cooperative-Control.pdf>. Luettu 31.10.2016.

3 Lightweight Access Point FAQ. 2010. Verkkodokumentti. Cisco Systems, Inc. <http://www.cisco.com/c/en/us/support/docs/wireless/aironet-1200-series/70278-lap-faq.html>. Päivitetty 21.1.2010. Luettu 31.10.2016.

4 Cisco Meraki Datacenter Design. 2016. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/trust#data-centers>. Luettu 14.6.2016.

5 Out of Band Control Plane. 2016. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/trust#oob>. Luettu 14.6.2016.

6 MR42 Datasheet. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/lib/pdf/meraki_datasheet_MR42.pdf>. Luettu 7.6.2016.

7 Cisco 802.11ac Wave 2 FAQ. 2015. Verkkodokumentti. Cisco Systems, Inc. <http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.html>. Luettu 24.11.2016.

8 Meraki MR SU-MIMO, MU-MIMO, and Beamforming. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Meraki_MR_SU-MIMO%2C_MU-MIMO%2C_and_Beamforming>. Luettu 24.11.2016.

9 Cisco ClientLink: Optimized Device Performance with 802.11n. 2009. Verkkodokumentti. Cisco Systems, Inc. <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/white_paper_c11-516389.html>. Luettu 24.11.2016.

10 Solutions: BOYD. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/solutions/byod>. Luettu 15.6.2016.

11 Cisco Meraki BOYD Solution. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/lib/pdf/meraki_byod_solution_guide.pdf>. Luettu 15.6.2016.

12 Enterprise Deployment Guide and Best Practices. Verkkodokumentti. Cisco Systems, Inc. < https://documentation.meraki.com/SM/Deployment_Guides/Enterprise_Deployment_Guide_and_Best_Practices#Profiles>. Luettu 23.7.2016.

13 Systems Manager Quick Start. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/SM/Systems_Manager_Quick_Start>. Luettu 23.7.2016.

14 Systems Manager Licensing. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/zGeneral_Administration/Licensing/Systems_Manager_Licensing>. Luettu 23.7.2016.

15 Configuration Settings. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/SM/Profiles_and_Settings/Configuration_Settings#WiFi>. Luettu 23.7.2016.

16 Air Marshal White Paper. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/lib/pdf/meraki_whitepaper_air_marshal.pdf>. Luettu 17.6.2016.

17 Technologies: Mesh Routing. Verkkodokumentti. Cisco Systems Inc. <https://meraki.cisco.com/technologies/mesh-routing>. Luettu 18.6.2016.

18 Mesh Networking. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Mesh_Networking>. Luettu 18.6.2016.

19 Location analytics (CMX). Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Monitoring_and_Reporting/Location_Analytics_(CMX)#Introduction_2>. Luettu 18.6.2016.

20 Technologies: RF Optimization. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/technologies/rf-optimization>. Luettu 20.6.2016.

21 Spectrum Analysis Overview. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Radio_Settings/Spectrum_Analysis_Overview>. Luettu 20.6.2016.

22 Technologies: Application QoS. Verkkodokumentti. Cisco Systems, Inc. <https://meraki.cisco.com/technologies/application-qos>. Luettu 20.6.2016.

23 Getting Started. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/Getting_Started>. Luettu 23.4.2016.

24 Organization Settings. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/zGeneral_Administration/Organizations_and_Networks/Organization_Settings>. Luettu 23.4.2016.

25 Packet Capture Overview. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Monitoring_and_Reporting/Packet_Capture_Overview>. Luettu 23.4.2016.

26 Navigating the Event Log. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MX-Z/Monitoring_and_Reporting/Navigating_the_Event_Log>. Luettu 23.4.2016.

27 PCI Compliance with Meraki. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Other_Topics/PCI_Compliance_with_Meraki#Meraki_PCI_Report_Tool>. Luettu 24.4.2016.

28 RF Spectrum Page Overview. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Monitoring_and_Reporting/RF_Spectrum_Page_Overview>. Luettu 24.4.2016.

29 Managing Dashboard Administrators and Permissions. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/zGeneral_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions#Managing_Network_Permissions>. Luettu 26.4.2016.

30 Wireless Encryption and Authentication Overview. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Encryption_and_Authentication/Wireless_Encryption_and_Authentication_Overview>. Luettu 26.4.2016.

31 Splash Page Overview. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Splash_Page/Splash_Page_Overview>. Luettu 27.4.2016.

32 Facebook Login. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Splash_Page/Facebook_Login>. Luettu 27.4.2016

33 Network Access Control (NAC). Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Network_Access_Control_%28NAC%29>. Luettu 27.4.2016.

34 Google Sign-In. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Splash_Page/Google_Sign-In>. Luettu 27.4.2016.

35 SSID Modes for Client IP Assignment. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Client_Addressing_and_Bridging/SSID_Modes_for_Client_IP_Assignment>. Luettu 30.4.2016.

36 Adult Content Filtering Overview. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Adult_Content_Filtering_Overview>. Luettu 30.4.2016.

37 Firewall Rules. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Firewall_Rules>. Luettu 30.4.2016.

38 Traffic and Bandwidth Shaping. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Traffic_and_Bandwidth_Shaping>. Luettu 30.4.2016.

39 VLAN Tagging. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Client_Addressing_and_Bridging/VLAN_Tagging>. Luettu 3.5.2016.

40 VLAN Tagging on MR Access Points. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Client_Addressing_and_Bridging/VLAN_Tagging_on_MR_Access_Points#Per-SSID_VLAN_tagging_in_Meraki_APs>. Luettu 3.5.2016.

41 Cheshire, Stuart. Zero Configuration Networking (Zeroconf). Verkkodokumentti. <http://www.zeroconf.org/>. Luettu 4.5.2016.

42 Bonjour Overview. Verkkodokumentti. Apple, Inc. <https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/NetServices/Introduction.html#//apple_ref/doc/uid/TP40002445-SW1>. Luettu 4.5.2016.

43 Configuring Bonjour forwarding for the MX security Appliance. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MX-Z/Other_Topics/Configuring_Bonjour_forwarding_for_the_MX_Security_Appliance>. Luettu 4.5.2016.

44 Cheshire, S. & Krochmal, M. Multicast DNS (RFC 6762). Verkkodokumentti. Internet Engineering Task Force (IETF). <http://www.ietf.org/rfc/rfc6762.txt>. Luettu 4.5.2016.

45 Bonjour forwarding. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Client_Addressing_and_Bridging/Bonjour_Forwarding>. Luettu 4.5.2016.

46 Band Steering Overview. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Radio_Settings/Band_Steering_Overview>. Luettu 7.5.2016.

47 Minimum Bitrate Control. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Radio_Settings/Minimum_Bitrate_Control>. Luettu 7.5.2016.

48 SNMP Overview and Configuration. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/zGeneral_Administration/Monitoring_and_Reporting/SNMP_Overview_and_Configuration>. Luettu 8.5.2016.

49 Real-Time Location Services (RTLS). Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Monitoring_and_Reporting/Real-Time_Location_Services_%28RTLS%29>. Luettu 8.5.2016.

50 Keyhole Markup Language. Verkkodokumentti. Google, Inc. <https://developers.google.com/kml/>. Luettu 8.5.2016.

51 Using the Dashboard XML API or Public Status Page. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Monitoring_and_Reporting/Using_the_Dashboard_XML_API_or_Public_Status_Page>. Luettu 8.5.2016.

52 SSID Availability. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Other_Topics/SSID_Availability>. Luettu 12.5.2016.

53 Bluetooth Low Energy (BLE). Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Bluetooth/Bluetooth_Low_Energy_(BLE)>. Luettu 12.5.2016.

54 Creating and Applying Group Policies. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Group_Policies_and_Blacklisting/Creating_and_Applying_Group_Policies>. Luettu 13.5.2016.

55 Using RADIUS Attributes to Apply Group Policies. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Group_Policies_and_Blacklisting/Using_RADIUS_Attributes_to_Apply_Group_Policies>. Luettu 13.5.2016.

56 Managing User Accounts using Meraki Authentication. Verkkodokumentti. Cisco Systems, Inc. <https://documentation.meraki.com/MR/Splash_Page/Managing_User_Accounts_using_Meraki_Authentication>. Luettu 13.5.2016.

57 AeroHive Deployment Guide. 2013. Verkkodokumentti. AeroHive Networks, Inc. <http://tln.lib.mi.us/dept/technology-services/wifi/files/aerohive/Aerohive%20Deployment%20Guide.pdf>. Luettu 27.6.2016.

58 HiveManager NG. Verkkodokumentti. AeroHive Networks, Inc. <http://media.aerohive.com/documents/Aerohive_Datasheet_HiveManager_NG.pdf >. Luettu 27.6.2016.

59 HiveManager NG Virtual Appliance. Verkkodokumentti. AeroHive Networks, Inc. <http://media.aerohive.com/documents/Aerohive_Datasheet_HiveManager-NG-Virtual-Appliance.pdf>. Luettu 27.6.2016.

60 Public or Private Cloud: The Choice is Yours. 2013. Verkkodokumentti. AeroHive Networks, Inc. <http://media.aerohive.com/documents/901259441_Aerohive-Whitepaper-Public-or-Private-Cloud.pdf>. Luettu 28.6.2016.

61 Controllers, Cloud, & Cooperative Control. 2015. Verkkodokumentti. AeroHive Networks, Inc. <http://media.aerohive.com/documents/1037869545_Aerohive-Whitepaper-Controllers-Cloud-Cooperative-Control.pdf>. Luettu 29.6.2016.

62 Cooperative Control Wireless LAN Architecture. 2012. AeroHive Networks, Inc. <http://media.aerohive.com/documents/524245518_Aerohive-Whitepaper-Cooperative_Control_Wireless_LAN_Architecture.pdf>. Luettu 29.6.2016.

63 How to Configure a GRE Tunnel. 2009. Verkkodokumentti. Cisco Support Community. Päivitetty 14.4.2014. <https://supportforums.cisco.com/document/13576/how-configure-gre-tunnel>. Luettu 29.6.2016.

64 Strong, Abby. What is a WLAN Controller (part 2). 2014. Hivemind Blog, AeroHive Boundless. <http://boundless.aerohive.com/blog/what-is-a-wlan-controller-part-2.html>. Luettu 29.6.2016.

65 AeroHive AP245X. Verkkodokumentti. AeroHive Networks, Inc. <http://media.aerohive.com/documents/Aerohive_Datasheet_AP245X.pdf>. Luettu 1.7.2016.

66 AeroHive AP250. Verkkodokumentti. AeroHive Networks, Inc. <http://media.aerohive.com/documents/Aerohive_Datasheet_AP250.pdf>. Luettu 1.7.2016.

67 AeroHive AP245X 802.11ac Wave 2 Wireless Access Point. Verkkodokumentti. AeroHive Networks, Inc. <http://www.aerohive.com/products/access-points/ap245x.html>. Luettu 1.7.2016.

68 AeroHive AP250 802.11ac Wave 2 Wireless Access Point. Verkkodokumentti. AeroHive Networks, Inc. <http://www.aerohive.com/products/access-points/ap250.html>. Luettu 1.7.2016.

69 Application Visibility and Control. 2012. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/pdfs/Aerohive-Solution_Brief-Application-Visibility-and-Control.pdf>. Luettu 1.7.2016.

70 RF-IQ. Verkkodokumentti. AeroHive Networks, Inc. <http://www.aerohive.com/solutions/technology/rf-iq.html>. Luettu 1.7.2016.

71 Assured Device and Data Security. Verkkodokumentti. AeroHive Networks, Inc. <http://www.aerohive.com/solutions/technology/assured-device-and-data-security.html>. Luettu 1.7.2016.

72 Wi-Fi Client Throughput—Maximized. Verkkodokumentti. AeroHive Networks, Inc. <http://www.aerohive.com/solutions/technology/maximizing-client-throughput.html>. Luettu 2.7.2016.

73 Configuring the Network Policy Information. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-the-network-policy-information.htm>. Luettu 4.7.2016.

74 Configuring Wireless SSID Settings. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-wireless-ssid-settings.htm>. Luettu 4.7.2016.

75 Configuring User Profile Settings. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-user-profile-settings.htm>. Luettu 4.7.2016.

76 Configuring User Profile Assignment. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-user-profile-assignment.htm>. Luettu 4.7.2016.

77 Configuring a User Group. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-user-group.htm?Highlight=group%20policy>. Luettu 4.7.2016.

78 Configuring User Groups. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-local-user-group.htm>. Luettu 4.7.2016.

79 Configuring AP Device Template. 2016. Verkkodokumentti. AeroHive Networks. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-ap-device-template.htm>. Luettu 8.7.2016.

80 Configuring Port Types. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-port-type.htm>. Luettu 8.7.2016.

81 Configuring a Radio Profile. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-radio-profile.htm>. Luettu 8.7.2016.

82 Configuring SSID Optional Settings. 2016. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-ssid-optional-settings.htm>. Luettu 8.7.2016.

83 Instant Overview. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/techdocs/Instant_40_Mobile/Advanced/Content/UG_files/Instant_overview/Instant%20Overview.htm>. Luettu 13.7.2016.

84 Channel Metrics. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/techdocs/InstantWenger_Mobile/Advanced/Content/Channel%20Metrics.htm>. Luettu 13.7.2016.

85 Virtual Controller. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/techdocs/InstantWenger_Mobile/Advanced/Content/Instant%20User%20Guide%20-%20volumes/Virtual%20Controller.htm#virtual_controller_3287683416_1026804>. Luettu 13.7.2016.

86 Aruba Instant Wi-Fi. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf>. Luettu 14.7.2016.

87 Aruba AirWave. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/assets/ds/DS_AW.pdf>. Luettu 14.7.2016.

88 AirWave 8.2 User Guide. 2016. Verkkodokumentti. Aruba Networks. Päivitetty 1.4.2016. <https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/21059/Default.aspx>. Luettu 14.7.2016.

89 Aruba Central User Guide. 2016. Verkkodokumentti. Aruba Networks. <http://help.central.arubanetworks.com/2.2.6/documentation/online_help/content/pdfs/aruba%20central%20user%20guide.pdf>. Luettu 17.7.2016.

90 Using the SCE and DPI in the Data Center. Verkkodokumentti. Cisco Systems, Inc. Päivitetty 29.8.2008. <http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/SCE_DPI.html>. Luettu 17.7.2016.

91 Viewing the Applications List and Launching the Application 360° View. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/viewing-applications.htm>. Luettu 17.7.2016.

92 Viewing the IP Firewall Policy List. Verkkodokumentti. AeroHive Networks, Inc. <http://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/viewing-ip-firewall-policy-list.htm>. Luettu 17.7.2016.

93 Aruba 330 Series Access Point. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/assets/ds/DS_AP330Series.pdf>. Luettu 18.7.2016.

94 Enhanced ClientMatch Technology. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/assets/tg/TB_EnhancedClientMatch.pdf>. Luettu 18.7.2016.

95 IP Nat Terminology and Considerations. Verkkodokumentti. Internet Engineering Task Force. <https://tools.ietf.org/html/rfc2663>. Luettu 16.8.2016.

Meraki auto RF

DATASHEET

Meraki Auto RF

Cloud-Based Spectrum Analysis and RF Optimization

As wireless networks assume a more critical role in the networking infrastructure, ensuring predictable performance becomes ever more important. However, the shared spectrum on which WiFi networks rely has become increasingly congested, both from other wireless networks and from non-WiFi sources like Bluetooth devices, cordless phones, and microwave ovens. Network administrators are often forced to choose between complex, costly RF management systems and suffering from unreliable wireless network performance. Meraki Auto RF provides a better alternative.

Meraki Auto RF is a powerful, yet completely automated RF optimization system that delivers hassle-free, high-performance WiFi, even under challenging interference conditions. With Auto RF, every access point on the network continuously and automatically monitors its surroundings for any source of interference that could affect WiFi performance. Interference metrics, including data from a powerful spectrum analyzer built into each Meraki AP, are uploaded to the Cloud Controller. Armed with real-time and historical data, the Cloud Controller continually assesses the health of the entire network, dynamically tuning wireless channel selection, transmit power, and client connection settings to automatically adapt to changing interference conditions.

Features

Spectrum Analyzer Detects Non-WiFi Interference

- Fine-grained data from dedicated spectrum analysis hardware on AP
- Quantifies interference from Bluetooth devices, microwave ovens, etc.
- Real-time spectrum visualization over the web
- Available on all Meraki 802.11n APs

802.11 Radios Monitor WiFi Environment

- 2.4 and 5 GHz 802.11 channel utilization
- Interference from neighboring APs
- Client device capabilities

Cloud-Based Algorithms Determine Optimal Configuration

- Utilizes real-time and historical data uploaded from APs
- Algorithms tuned with inputs from 15,000+ networks
- Administrators can chose how often scans and replanning takes place

Performance Settings Tune Automatically

- Channel assignment
- Per radio transmit power
- Band steering – move capable devices to 5 GHz

High-resolution spectrum analysis